Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7 – No. 25, January 2019 – www.caeaccess.org

PA-AKA: Privacy-Aware and Lightweight Authentication Scheme for Long Term Evolution (LTE)

Olakanmi O. Oladayo
University of Ibadan
Office 6, Electrical and Electronic Engineering Department

Eleshinnla Adebola
University of Ibadan
Security & Embedded Systems Research Laboratory

Dada Adedamola
University of Ibadan
Security & Embedded Systems Research Laboratory

ABSTRACT
Several authentication schemes had been proposed for LTE to ensure confidentiality between the authorised users and the network. Most of these schemes could not preserve users' privacy especially during the initial connection, although, few that are able to preserve subscribers' identities completely left out Mobile Management Entity (MME) during International Mobile Subscriber Identity (IMSI) exchange. The inherent isolation of MME makes it impossible for MME to link pseudonym with identity in the subsequent connection.

In this work an improved privacy aware authentication scheme is proposed, which does not only preserve the subscribers' privacy during initial connection but allows MME to generate and map subscriber pseudonym with its identity in order to use pseudonym for subsequent connections. Thus, reduces computational overheads by reducing number of authentication operations performed by MME. A key-cluster based matrix approach was adopted at the Home Subscriber Server (HSS) to speed up the identification of subscribers.

General Terms
Mobile communication, security, LTE

Keywords
Security and privacy, subscriber, shared key, protocol, LTE

1. INTRODUCTION
LTE is referred to as a wireless broadband, it is an efficient transition towards a more advanced increase in capacity and speed of wireless data networks. That is, an advanced network beyond the 3G network that is capable of supporting a high demand for connectivity of devices. LTE accommodates more subscribers, who need to interact with other components such as Mobile Management Entity (MME) and Home Subscriber System (HSS). These components contain sensitive information that need to be secured through efficient security and access control scheme.

Efficient authentication between User Equipment (UE) and HSS is one of the major challenges of LTE protocols. For example some of the existing protocols present identity of UE as a plain text during the initial connection authentication, which makes user susceptible to any form of privacy attacks. To prevent this, authors in [1] and [2] proposed the use of Globally Unique Temporary Identity (GUTI), which is generated and mapped to IMSI of the user by MME for subsequent connections. However, their schemes bypassed MME during the exchange of IMSI in the initial connection, this implies that the MME would not have the knowledge of the user's IMSI, therefore, unable to generate and map GUTI to subscriber's identity. Apart from these two challenges, using key to locate the identity of subscriber by HSS may become computationally exhaustible for the HSS as the number of the subscribers increases.

To overcome these challenges, we proposed a privacy aware scheme for LTE that can be used in place of the existing schemes proposed in [1] and [2] for an effective authentication and key agreement in LTE. The proposed scheme, called Privacy Aware Authentication and Key Agreement (PA-AKA), provides an alternative way of identifying the subscriber alongside with his/her shared key using cluster based key-matrix to enhance searching speed of HSS. During the initial connection, IMSI is blinded using subscriber's key position identifier and the shared secret key in order to prevent the privacy issue associated with initial connection. To solve the isolation problem in the subsequent connections, the proposed scheme uses elliptic based parameters exchange technique to securely exchange the IMSI of the subscriber with MME.

The rest of the paper is organized as follows; section II contains the review of the related work, in section III, we examine the existing authentication and key agreement protocol of LTE, their problems and our contributions, section IV describes the methodology of the proposed scheme, the proposed scheme is analysed and compared with two existing schemes in terms of their computational overheads in section V, while conclusion is drawn in section VI..

2. RELATED WORK
In contrast to the circuit switched model of previous cellular systems, LTE has been designed to support only packet switched services. LTE provides seamless Internet Protocol (IP) connectivity between user equipment (UE) and the Packet Data Network (PDN), without any disruption to end users application during mobility [5]. In mobile communications, privacy is one of the major challenges, although many schemes and protocols have been proposed to preserve privacy in mobile communications.

For examples, the works in [11], [9], [7], and [8] are centered on different privacy and security schemes and protocols for mobile communications. Author in [4] proposed a lightweight scheme to achieve data integrity and data confidentiality. The scheme involves a novel authentication and key agreement protocol for device to device communications. Warda et al. [3] examined flaws in some of the existing schemes and proposed a replacement for the backup procedure of identity presentation in the existing LTE protocol. Although their scheme was able to preserve subscribers privacy issue but the scheme could not solve the problem of inability of new MME linking GUTI of subscriber with its IMSI during roaming. Also, their scheme consumed more power and memory.

Zather et al. [12] proposed a new scheme to resolve privacy issue associated with the transmission of subscriber's IMSI as a plain text and prevent mobility management attacks. Public key cryptography was used to encrypt the messages in transit and the RSA was used to compute a temporary value for the IMSI so as to send it as a challenge to the HSS. However, this scheme is not resistant to some of the attacks related to key collision, and has much memory overhead and high computational power.

Group based communications faces new challenges like effective authentication during roaming, users will be delayed thereby increasing communication overhead, and privacy of the users will become prone to attack. To solve this, Chengzhe [13] proposed a scheme with a novel group authentication. In the scheme, a privacy aware security approach was used to securely transmit the real identities of users, and the use of pseudonym by UE in the initial connection to access the LTE network. A key was generated by the scheme through the challenge response in order to encrypt and transmit the real identity.

3. PRELIMINARY

Figure 1 depicts the security architecture of the LTE in a simplified mode. Each subscriber registers with the nearest Home Network (HN) with his/her details stored in the HSS. The UE connects with MME through the Evolved Nodeb (eNb). The eNb is an enhanced base transceiver station performs radio resource management. The UE and HSS use the MME as the authenticating equipment, the UE sends it request via MME to HSS. There are two levels of security in the LTE protocol; Access Stratum and Non-Access Stratum. The access stratum protects the signaling and user planes between UE and eNb while the non-access stratum protects the control plane between UE and MME.

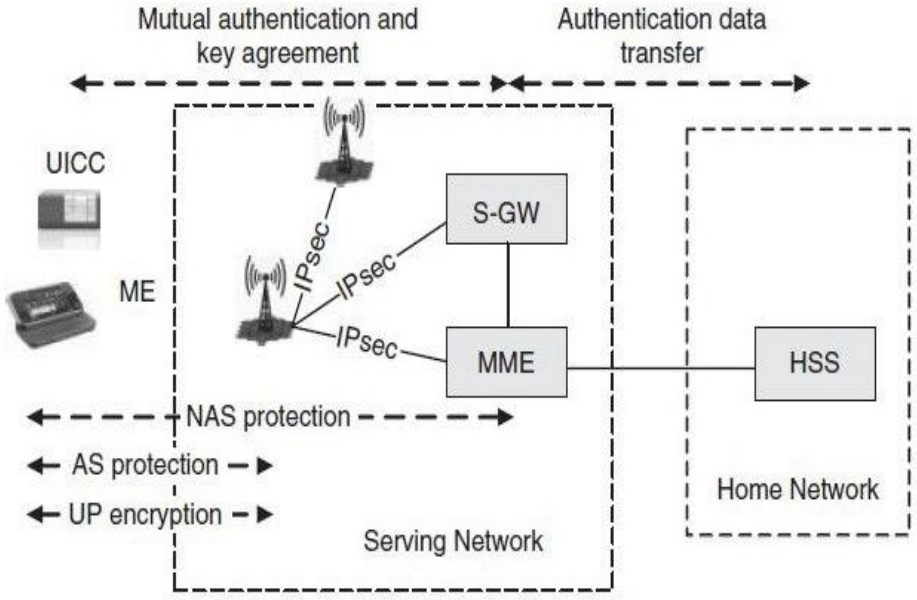

Fig 1: A simplified LTE Security Architecture

3.1 Evolved Packet System Authentication and Key Agreement (EPS-AKA)

EPS-AKA is the authentication and the key agreement technique used in LTE security as defined in TSA 33.401 [1]. To execute this protocol EPS-AKA, a shared secret key k, IMSI and a set of hash functions f_0 - f_5 are stored on the UE and HSS to ease authentication and key agreement. The authentication in EPS-AKA for LTE is briefly described below:

3.1.1 The Initial Connection

The UE initiates the authentication with HSS by sending its request with its IMSI through the following steps:

- The UE initiates the authentication with HSS by sending its request with its IMSI to MME, who then sends the received UE's IMSI and its identity to HSS.
- On the crest of the request, the HSS then computes the Evolved Packet System Authentication Vector EPS-AV as follows:
  - RAND = f_0(seed), where RAND is the 128-bit randomly generated number.
  - MAC = f_{1k}(SQN||RAND||AMF), where AMF is the Authentication and Key Management Field, SQN is the Sequenced number maintained at the HSS and MAC is the Message Authentication Code.
  - XRES = f_{2k}(RAND), XRES is the expected response and secret key k was the shared secret key k between UE and HSS.
  - CK = f_{3k}(RAND), CK is the Cipher Key.
  - IK = f_{4k}(RAND), IK is the integrity Key.
  - AK = f_{5k}(RAND), AK is the Anonymity Key.
  - AUTN = SQN $\oplus$ AK||AMF||MAC), AUTN is the Authentication Token.
  - KASME = KDF(CK, IK, MME_{id}), K_{ASME} is Access security Management Entity.
  - EPS-AV = (RAND||AUTN||XRES||K_{ASME}).
- HSS responds back with the requested authentication vector EPS-AV to MME.
- MME then extracts RAND and AUTN from the authentication vector, HSS responded with and then

forwards it to UE as a trial. KSI_{ASME} would be sent alongside the trial, this is majorly for UE and MME to identify K_{ASME} without starting another authentication procedure.

- UE then computes AK and extract SQN from the AUTN forwarded to him, he computes MAC' and compares if MAC' is equal to MAC in AUTN sent, if AUTN is acceptable UE computes RES as RES = f_{2k}(RAND) and responds with a user authentication response message and compute CK, IK, and K_{ASME} but if not equal its sends a reject failure message to MME stating reasons for such response.
- MME compares RES and XRES, if equal the authentication is successful otherwise sends a reject failure message to UE.

Then, a key K_{ASME} would be shared between UE and MME. Some hierarchy of keys are then generated from the shared key K_{ASME} to be used for protection of NAS and AS. MME then allocates a temporary new identifier called GUTI to UE. Until NAS security is activated a new GUTI will not be sent to UE.

3.1.2 Subsequent Connections

During subsequent connections, UE is identified by transmitting a GUTI, K_{ASME} is also send along with the request. On the crest of the connection request, MME identifies K_{ASME}

corresponding to the GUTI received alongside K_{ASME}. The security of the message is checked and MME decides if to reuse the K_{ASME} computed during the initial connections or to restart the EPS-AKA, MME locates the identity of UE in its local database through the IMSI-GUTI mapping and continues in the mode as it was in the initial connections. Connections requests can be authenticated using the K_{ASME} without performing a fresh EPS-AKA, several connections can be authenticated with a new set of security keys re-derived from K_{ASME}.

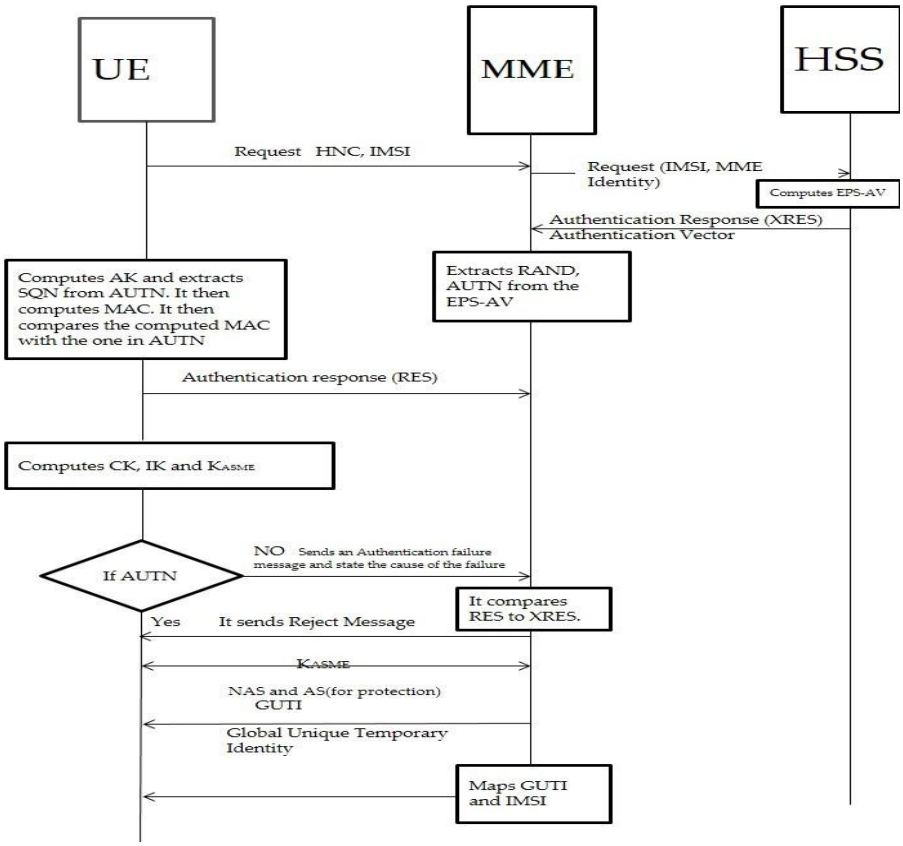

Fig. 2. EPS-AKA during initial connections of an LTE Security Architecture

Table I: Symbols and Notations

System	Notation
LTE	Long Term Evolution
EPS-AKA	Evolved packet System Authentication and Key Agreement
PA-AKA	Privacy Aware Authentication and Key Agreement
T_{id}	Temporary Identity of UE
KPI	Key Position Identifier
H	One-way collision-resistant hash function
κ	Shared Key
UE	User Equipment
MME	Mobile Management Entity
HSS	Home Subscriber System

3.2 Problems and Our Contributions

Non preservation of privacy of subscribers is the major flaws of the procedure described in the preliminary section. To avoid tracking of profile, the IMSIs of subscribers should be protected otherwise it will create an avenue to monitor the subscriber from time to time by adversary. EPS-AKA scheme used a pseudonyms called GUTI to preserve the IMSIs of

subscribers during subsequent connection requests. It allows MME to create and use GUTI during subsequent connection, which is the major reason why subscribers' IMSIs must be sent to MME during the initial connection. However, an adversary acting as MME can take advantage of this by requesting for IMSI of the subscriber who roams in the new MME's environment. Apart from this, a new MME, in a newly visited network, may not be able to retrieve the IMSI of the subscriber from its GUTI, thereby hinders authentication with HSS. Another performance bottleneck is the delay overhead incurs by HSS in locating subscriber's information in its large database after a successful authentication. All these flaws and shortcomings as noted in initial and subsequent connections are solved in the proposed scheme.

4. PROPOSED PA-AKA SCHEME

The key management of this scheme is similar to that of EPS-AKA except that subscribers' keys in HSS are partitioned into a matrix-like clusters called Key Cluster Matrix (KCM), as shown in Figure 3, and the privacy of UE is preserved during the initial connection by generating temporary identity for UE.

In the improved initial connection authentication, UE computes and sends a temporary pseudonym T_{id} and blinds subscriber key's position b to MME. This is to protect the UE's privacy and secure the key during the initial connection. MME then forwards its identity, received T_{id} and b to the HSS, who responded by computing the authentication vector (as described in the key management phase of EPS-AKA) to MME. MME then extracts authentication parameters (RAND, AUTN) and forwards it to UE, who uses them to ascertain the received Message Authentication Code (MAC). It then computes its response (RES), and sends it to MME who validate it by comparing it with the expected response (XRES). The blinded Key Position Identifier(KPI), b contains the row and column indices of the subscriber key in the KCM of HSS, is forwarded to HSS through MME. SS unblinds the received b in order to extract KPI of the subscriber key in KCM. The KPI is then use to locate the subscriber's key in KCM.

To solve the problem of isolation of MME during the initial connection's IMSI exchange, we introduced a 2-way key exchange mechanism to facilitate a secured IMSI exchange between HSS and MME. Thus, solve the isolation problem observed in [2] scheme. Once MME get the IMSI, it can then generate a permanent pseudonym GUTI for subsequent connections of UE. The proposed scheme consists of two stages; initial connection and subsequent connections that are depicted in Figure 4 and fully described below.

4.1 Improved Initial Connection

Initial connection improved on the initial connection of the schemes in [2], all the operations in EPS-AKA key management with protocol are adopted except that temporary GUTI, T_{id} and blinded cluster identity are added to solve initial connection privacy issue. The improved initial connection operation is summarized below;

- UE computes a temporary pseudo-identity T_{id} for the initial connection as:
  $T_{id} = (IMSI \oplus \kappa \oplus KPI)$
  where κ is the shared key of the subscriber.
- UE also blind its KPI as:
  $b = (KPI_{row}||KPI_{col} \oplus SQN)$

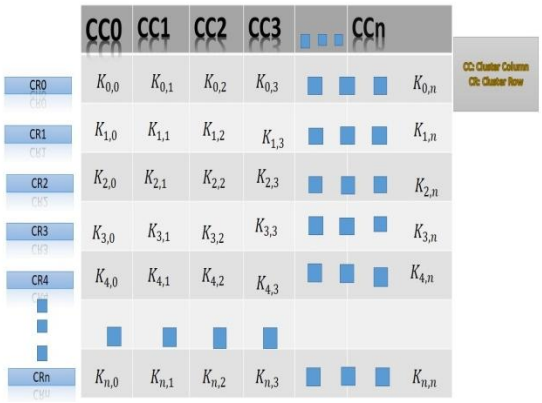

Fig 3: Key Cluster-Based Matrix

- It then sends a connection request that consists of T_{id} and b to MME. MME forwards the received request and its identity MME_{id} to HSS.
- Then continue the authentication procedure of EPS-AKA as described in section 3.1 to complete the initial connection authentication.
- HSS on receiving T_{id} and b, it unblinds KPI as:

  $KPI = KPI_{row}||KPI_{col} = KPI_{row}||KPI_{col} \oplus SQN \oplus SQN$), and uses the KPI to locate the UE's key in KCM. Once the key κ is retrieved, HSS unblinds the received temporary pseudo-identity to extract the UE's IMSI as:

  $$IMSI = T_{id} \oplus \kappa \oplus KPI$$

4.2 Improved Subsequent Connections

During subsequent connections, the MME needs the UE's IMSI, which is not catered for by the schemes [2] and [1]. Apart from this, in EPS-AKA any attempts to change MME during roaming, gives the new MME subscriber's GUTI without the UE's IMSI, therefore making authentication impossible [1]. To resolve these challenges, we proposed a mechanism for secure exchange of IMSI between old and new MMEs, new MME and HSS of EPS-AKA scheme in [1] and the scheme in [2].

4.2.1 2-way parameters' exchange

To solve the problem of MME being isolated during the initial connection's IMSI exchange and roaming. We proposed a 2-way parameter's exchange mechanism to securely exchange IMSI between MME and HSS. The mechanism is described below:

- MME randomly generates $\delta \in Z_p^*$ and computes

  $W_{mme} = \delta * XRES$;
- HSS also selects a random $\beta \in Z_p^*$, computes $W_{hss} = \beta * RES, q_{hss} = W_{hss} * P$ and publishes q_{hss} as its 2way public key.
- MME then computes $q_{mme} = W_{mme} * P$, publishes q_{mme} as its 2-way public key, and computes the shared exchange key γ as $\gamma = \delta * q_{hss}$
- HSS also computes the shared exchange key γ as $= \beta * q_{mme}$. HSS then encrypt and sends the UE's IMSI to MME, using its shared exchange key , who decrypts it using its own shared exchange key

γ. MME can generate GUTI for UE and maps it with its IMSI. Thus, solving the problem of secure exchange of IMSI with new MME during GUTI generation.

5. PERFORMANCE EVALUATION

In this section, we evaluated the performance of the proposed scheme in terms of computational and storage overheads.

5.1 Computational Overhead

We compared the computational overheads of UE and HSS of the proposed scheme with that of two LTE's schemes in [1] and [2]. To achieve this, we simulated the computational overheads of the three schemes using the computational cost of all the cryptographic operations as shown in Table II. The following notations are used to represent the cryptographic operations used in the simulation.

1) T_{xor}: The execution time of an XOR operation.
2) T_{hash}: The execution time of a SHA-256 hash function.

Table III shows the computational overheads of all the three LTE schemes. Figure 5 and 6 show the computational overhead incurred by UE and HSS of each of the schemes. Figure 5 shows that the UE of the scheme in [2] has the highest overhead while the proposed and [1] schemes' UEs incurred the same overhead. Also, Figure 6 depicts the overheads incurred at HSS, the HSS of the scheme in [2] incurred the highest overhead compared to the proposed and [1] schemes. These indicate that the proposed scheme not only solves the privacy problem during initial connection but securely provides IMSI to both old and new MMEs during the subsequent connection without incurring extra computational cost.

5.2 Space Overhead

We also evaluate the proposed scheme based on required memory space by comparing its storage overhead with that of [2], who HSS also uses key to locate IMSI. We observed that the proposed scheme requires lesser memory space than [2]. The amount of space needed in the random access memory and read only memory at the UE, MME and HSS is presented in Table IV.

5.3 Security Analysis

In this section, we show how the scheme is capable of thwarting some of the common attacks in LTE, therefore validate the security efficiency of the scheme

a. Eavesdropping attack is a common attack in LTE, involves secretly listening to the subscribers' private parameters exchange during registration session. This is possible since UE and MME are connected together through a wireless link, which is prone to eavesdrop. To thwart this, all the initial connection's sensitive parameters such as IMSI and KPI are symmetrical encrypted as $T_{id} = (IMSI \oplus \kappa \oplus KPI)$ and $b = (KPI_{row}||KPI_{col} \oplus SQN)$. Thus, eavesdropper would only get blinded personal details of the subscriber.

b. Denial of Service (DoS): DoS involves making network resources unavailable to the targeted subscribers. This type of attack involves sending superfluous requests in an attempt to overflow the traffic along the targeted subscriber, thereby affecting legitimate request from being considered. The proposed scheme provides a secure mechanism which involves verification of IMSI, shared key κ and KPI, therefore without the knowledge of these parameters adversary cannot communicate with HSS through MME, thus DoS cannot be launched.

c. Replay attack: Replay attack is a form of attack where subscriber data transmission session parameter is copied and then later used to initiate another illegal session with MME. In PA-AKA, b is stamped with unique SQN as $b = KPI_{row}||KPI_{col} \oplus SQN$. If an adversary tried to reused T_{id} and b, the current SQN with the HSS would not give correct IMSI and KPI. Thus prevents replay attack. Forward security is also guarantee since SQN changes at every connection, therefore adversary cannot access personal parameters of UE with previous SQN.

6. CONCLUSION

In this paper, we proposed an improved privacy aware scheme which is not only efficient but preserves the privacy of subscriber during connections. This was not taken care off in EPS-AKA scheme. Also, the proposed scheme unlike the scheme in [2], securely provides subscriber's IMSI for the mapping of GUTI and IMSI during subsequent connections.

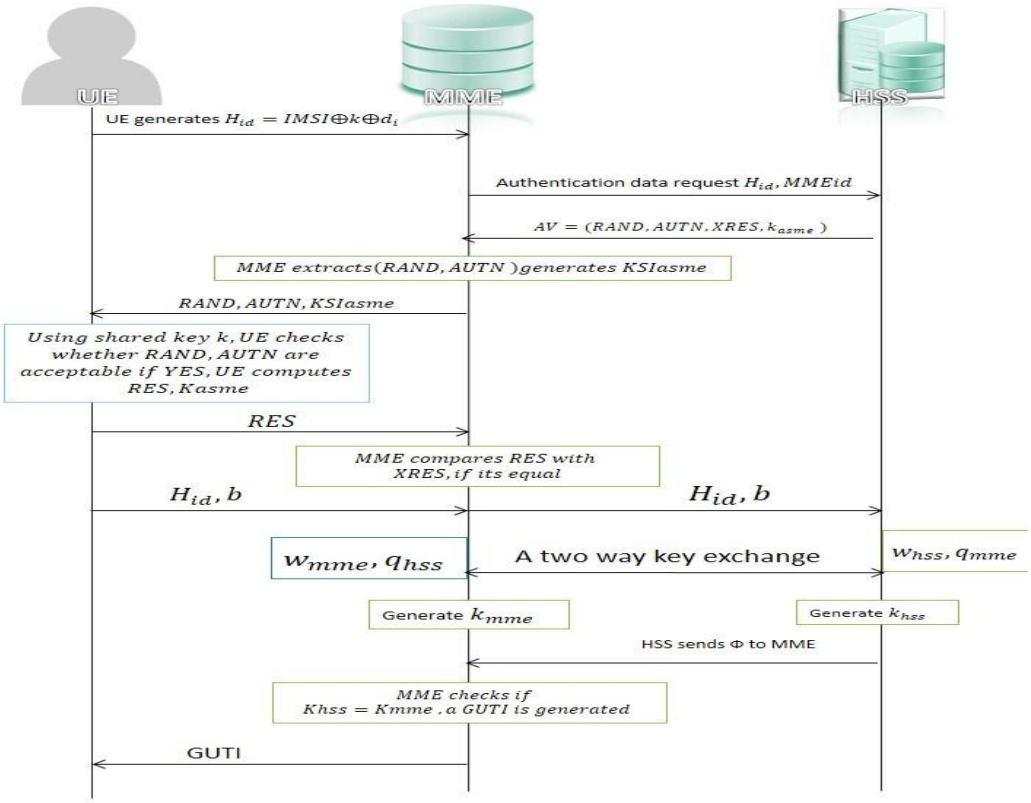

Fig 4: A lightweight PA-AKA scheme during initial connections of an LTE

Table II: Computational Overhead of various cryptography operations [16]

Cryptographic operations	Execution time (ms)
Thash	0.56
Txor	1×10^{-6}

Table III: Computational Overhead of the three schemes

Cryptographic operations	EPS-AKA[1]	Hiten Choudury[2]	Proposed Scheme
UE	$6Thash + 1Txor$	$7T_{hash} + 1Txor$	$4Txor + 6T_{hash}$
MME	$2Thash$	$2Thash$	$1Txor + 2T_{hash}$
HSS	$6Thash + 1Txor$	$(N+7)T_{hash} + 1Txor$	$5Txor + 6T_{hash}$
Total Execution(ms)	7.36	564	7.36

Table IV: Storage Overhead

Entities	Hiten Choudury Scheme[2]	Proposed Scheme
UE	128bits to temporarily store r and b respectively	128bits to temporarily store T_{id} and b respectively
MME	128bits to temporarily store r and b respectively	128bits to temporarily to store T_{id} and b
HSS	128bits to permanently store KSI	128bits to permanently store KPI
Additional Memory Space	64bytes in RAM and 32bytes in ROM	32bytes in RAM and 16bytes

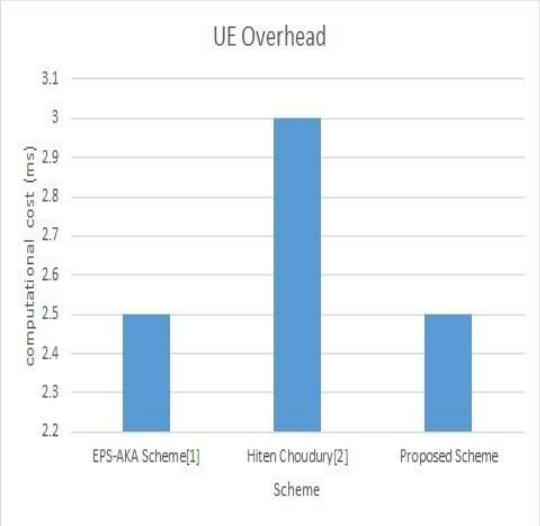

Fig. 5. Computational Overhead of UE for different Schemes

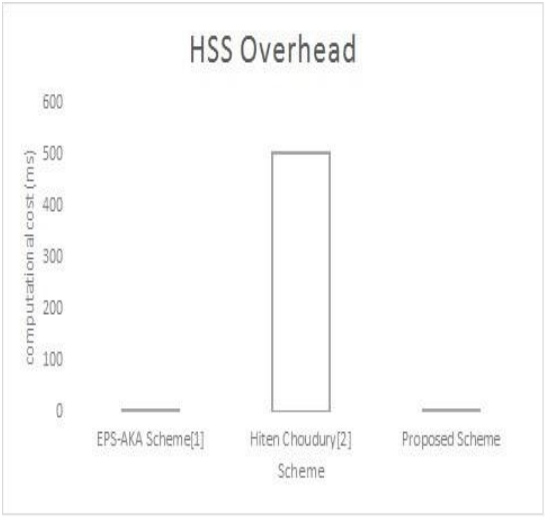

Fig. 6. Computational Overhead of HSS for different Schemes

7. REFERENCES

[1] 3GPP, 3GPP System Architecture Evolution (SAE); Security architecture," 3rd Generation Partnership Project (3GPP), TS 33.401, 2011.[Online]. Available: http://www.3gpp.org/ftp/Specs/html-info/33401.htm

[2] Hiten Choudhury (2016). A Computationally Light Scheme for Enhanced Privacy in LTE. International Conference to Digital World.

[3] Warda Ahmed, Sidra Anwar and M. Junaid Arshad (2016). Security Architecture of 3GPP LTE and LTE-A Network. International Journal of Multidisciplinary Sciences and Engineering, Vol. 7, No. 1.

[4] Soran Hussein (2014). Lightweight Security Solutions for LTE/LTE-A Networks. Networking and Internet Architecture. Universite Paris Sud - Paris XI.

[5] P.Lescuyer, and T.Lucidarme. Evolved Packet System (EPS): The LTE and the SAE Evolution of 3G UMTS.

[6] Uijin Jang, Hyungmin Lim and Hyungjoo Kim (2014). Privacy-Enhancing Security Protocol in LTE Initial Attack. Symmetry, Special Issue Applied Cryptography and Security Concerns based on Symmetry for the Future Cyber World.

[7] N. Asokan (1994). Anonymity in a mobile computing environment, in IEEE Workshop on Mobile Computing Systems and Applications, Santa Cruz, CA, pp. 200204.

[8] H. Y. Lin and L. Harn (1995). Authentication protocols for personal communication systems, ACM SIGCOMM Computer Communication Review, vol. 25(4), no. 4, pp. 256261.

[9] J. Park, J. Go, K. Kim, B. A, C. B, and D. C. (2001) Wireless authentication protocol preserving user anonymity, in Symposium on Cryptography and Information Security, Oiso, Japan, pp. 159164.

[10] A. Shabut, K. Dahal and I. Awan (2013). Enhancing dynamic recommender selection using multiple rules for trust and reputation models in MANETs. IEEE 25th international conference on tools with artificial intelligence, pp. 654-660

[11] M. Barbeau and J. M. Robert (2005). Perfect identity concealment in UMTS over radio access links, in IEEE International Conference on Wireless and Mobile Computing, Networking and Communications Montreal, Canada, pp. 7277.

[12] Zaher Jabr Haddad, Sanaa Taha and Imane Aly Saroit Ismail (2014). SEPS-AKA: A Secure Evolved Packet System Authentication and Key Agreement Scheme for LTE-A Networks. The Sixth International Conference on Wireless & Mobile Networks.

[13] Chengzhe Lai, Hui Li , Rongxing Lu, Xuemin (Sherman (2013). SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. The International Journal of Computer and Telecommunications Networking archive Volume 57 Issue 17,Pages 34923510

[14] Mohammed Ramadan, Guohong Du, Fagen Li and Chunxiang Xu (2016). A Survey of Public Key Infrastructure-Based Security for Mobile Communication Systems. Symmetry, Special Issue Symmetry in Secure Cyber World.

[15] D. Boneh and M. Franklin (2001) Identity-based encryption from the weil pairing. Advances in cryptology-CRYPTO 2001, pp. 213-229.