Enhanced Authentication and Key Agreement Procedure of next Generation 3GPP Mobile Networks

Masoumeh Purkhiabani and Ahmad Salahi

Abstract—**In the next generation mobile networks, because of fundamental changes with respect to previous cellular 3.xG networks and integration different access network which caused frequent handover and provision all IP packet-based services, load transaction overhead such as authentication traffic overhead as an important initial security process to identity of users, between entities are a lot. In this research first explain evolved authentication and key agreement protocol for next generation Long term evolution/ System Architecture Evolution(LTE/SAE)networks and compared its enhancements with contrast to Universal Mobile Terrestrial System- Authentication and Key Agreement(UMTS-AKA), then, offers a new improvement protocol which increases performance of authentication procedure. The current 3GPP LTE –AKA has some shortcomings, including bandwidth consumption between a serving networks and a user's home network, computation overhead and imperfect mutual authentication. in fact the new proposed protocol by sharing serving network with Home Subscription Server(HSS) for execution of authentication procedure and increasing a little computation in Mobility Management Entity(MME) and generated joined authentication vectors in both MME and HSS can remove aforementioned problems during authentication process. The proposed scheme is analyzed and its advantages have been verified by simulation. Our new proposed protocol can satisfy security requirements and simulation result shows in the proposed-AKA with contrast to original-AKA, the more MS and service request rate, the more considerable deduction of authentication load for HSS.**

Index Terms— **LTE/SAE, UMTS-AKA, HSS, MME.**

I. Introduction

LTE project aims to ensure the continued competitiveness of 3GPP technologies for the future. Its objective is to develop a framework for an evolution or migration of 3GPP system to higher –data- rate, lower-latency, packet-optimized system, multiple Radio Access Technologies (RATs). In addition to LTE, 3GPP has specified flat IP-based network architecture as part of the system architecture evolution (SAE) effort [1]. EPS represents the very latest evolution of the UMTS standard and LTE, which dedicated to the evolution of the radio interface, and SAE which focuses on core network architecture evolution. The SAE/LTE architecture aims at integrating multiple wireless network technologies to deliver secure services to users. The rapid growth of mobile networks enables convenient access to integrated services such as the voice, data, and multimedia. In order to provide secure services over wireless networks with high QoS, security mechanisms such as authentication and encryption are deployed. EPS provides security feathers in a similar way as UMTS and GSM. As one of the most widely used security mechanisms, authentication is a process to identify a mobile user.

Considering the large changes made in the mobile network 3.xG, one of the main issues in these networks is discussion of security against various threats, which by progress and increase the growing complexity of networks and entry various services such as new multimedia services, Internet and e-commerce features, tried to improve the security mechanism. For instance, one of the most evolved security mechanisms is authentication and key agreement protocol (AKA) in 3.xG mobile networks which have been mutual. During the AKA protocol, parties (user and network) authenticate each other and agreed on the encryption and integrity keys, by the specific and complex mechanisms and algorithms (function f).Also, during authentication process in next generation mobile networks, key separation and key hierarchy has been added. Because of the importance of authentication protocol in the access network, to be more complex in terms of computational, and increasing different types of traffics (voice, data and multimedia) as well as integration of various networks and following that, increased traffic due to added handover between different networks and within a network as one of the authentication trigger on the access network, the authentication signalling overhead volume has been very high. So in terms of evaluation authentication protocol traffic in next generation mobile networks (LTE) and finding ways to improve the efficiency of mobile networks in terms of traffic overhead and decrease traffic without damage to network security is very important. Therefore, in this paper after research of the standard EPS-AKA authentication protocol in the LTE network, to improve its performance in terms of efficient use of bandwidth, and decrease wasted computation overhead, an improved protocol is recommended. The proposed protocol follows not only the security framework of the standard protocol, but also even in some security cases works better. In compare of the standard protocol, the quantity of improvement of proposed protocol is calculated and presented by computer software. A few research have been proposed to study the effect of number of authentication vectors [2] [3], the waiting probability of a new authentication vector [4], and the time interval needed to maintain an unused authentication vector [5]. Yan Zhang pointed out that a subsequent authentication event after all previous authentication vectors have been used must wait

Manuscript received August 20, 2011; revised October 27, 2011.

Masoumeh Purkhiabani is with Department of Electrical Engineering Islamic Azad University South Tehran Branch,Tehran,Iran

Ahmad Salahi is from Iran Telecommunication Research Center, Tehran, Iran

until the authentication vector arrays have been fetched from the authentication server[4].The authors showed that their proposed pre-authentication scheme decreases the authentication delay with minor increased signaling overhead. In 2005, Huang and Li introduced the X-AKA protocol [6] to overcome the program of low bandwidth consumption. In this protocol, the MS's HE distributes a TK (temporary key) to SN. This is different from the original method in that the HE calculates n-sets of AV and passes them to the SN. A TK is much smaller than n-sets of AV, and therefore it can save bandwidth consumption. It is noted that all computation in HE transfer to SN, so SN may not be able to afford complex computations with the current equipment.

In 2006, Al-Saraireh and Yousef suggested a new AKA protocol, which include reducing the number of messages transmitted between mobile phones and authentication center. In that protocol, AVs are not generated by the HE but instead the MS sends the authentication token via SN to the HE. So, signaling messages between the mobile network entities are reduced, but the new protocol showed two mistakes. One is that the MS must save n-sets of AV s on a limited space in MS. The other mistake is that each authentication SN must pass the authentication token back to the HE. This will cause delay in authentication [7].

The remainder of the paper is organized as follows: Section II describes the LTE/SAE networks and EPS AKA protocol and analyzed it in contrast with 3G UMTS. In Section III, described a new proposed AKA protocol. The simulation result is shown in Section 4. The paper is concluded in Section 5.

II. EPS System Architecture and EPS-AKA Mechanism

An LTE/SAE architecture that applies IP-based mobility control technology has two components: the access network and the core network. The access network is called the evolved universal terrestrial radio access network (E-UTRAN), based on orthogonal frequency-division multiplexing (OFDM) and single-carrier frequency-division multiple access (SC-FDMA) technologies and the core network is called the evolved packet core (EPC) which is different from UMTS core network, is shown in Fig.1. in addition to fundamental entities in core network, specified by GPRS[8], SAE comprises Mobility Management Entity(MME) , Serving Gateway (S-GW), Packet Data Network-Gateway(P-GW) and Policy and Charging Rules Function(PCRF).

The MME manages limitation protocols on the control plan such as, UE ID allocation, security, authentication, as well as the roaming control. The UPE (User Plan Entity) manages protocols on the user plane such as, storing UE contexts, terminating IDLE-state on the user plane, and context encryption. The S-GW manages mobile services between 2G/3G access and LTE access. In fact The MME and S-GW accommodate the LTE eNodeB (eNB) access system base stations. And finally, the P-GW manages mobile services between 3GPP access and non 3GPP access (such as WLAN and WiMAX).

P-GW is connection point for data networks that are outside the core network, such as the IMS, and accommodates3GPP access and non-3GPP radio access. PCRF controls QoS and charges, etc. In E-UTRAN, all radio access protocols must be managed in one node, namely eNodeB. Before a user is granted access to a network, *authentication* in general has to be performed. During authentication the user proves that he or she is the one he/ she claims to be. Typically, *mutual authentication* is desired, where the network authenticates the UE and the UE authenticates the network. Authentication is done with a procedure where each party proves that it has access to a secret known only to the participating parties, for example, a password or a secret key. It was clear from the start of the standardization process that E-UTRAN should provide a security level, at least as high as that of UTRAN. Access security in E-UTRAN therefore consists of different components, similar to those that can be found in UTRAN:

- Mutual authentication between UE and network.
- Key derivation to establish the keys for ciphering and integrity protection.
- Ciphering, integrity and replay protection of NAS signalling between UE and MME.
- Ciphering, integrity and replay protection of RRC signalling between UE and eNB.
- Ciphering of the user plane. The user plane is ciphered between UE and eNB.
- Use of temporary identities in order to avoid sending the permanent user identity (IMSI) over the radio link.

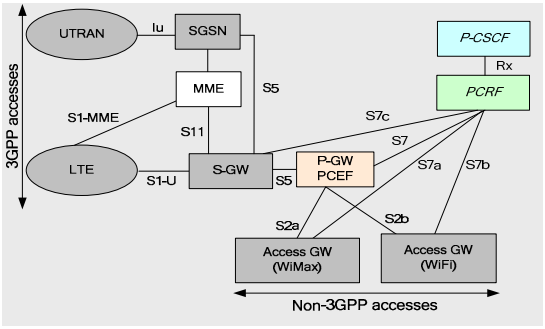


Fig.1. LTE/SAE architecture [9]

Mutual authentication in E-UTRAN is based on the fact that both the USIM card and the network have access to the same secret key K. This is a permanent key that is stored on the USIM and in the HSS/AuC in the home operator's network. Once configured, the key K never leaves the USIM or the HSS/AuC. The key K is thus not used directly to protect any traffic and it is also not visible to the end-user. During the authentication procedure, other keys are generated from the key K in the terminal and in the network that are used for ciphering and integrity protection of user plane and control plane traffic. For example, one of the derived keys is used to protect the user plane, while another key is used to protect the NAS signalling.

One reason why several keys are produced like this is to provide key separation and to protect the underlying shared secret K. In UTRAN and GERAN, the same keys are used for control signalling and user traffic, and hence this is also an enhancement compared to these earlier standards. This is, however, not the only key management enhancement as will be discussed below. The mechanism for authentication as

well as key generation in E-UTRAN is called EPS Authentication and Key Agreement (EPS AKA). Mutual authentication with EPS AKA is done in the same manner as for UMTS AKA, but as we will see when we go through the procedure, there are a few differences when it comes to key derivation. EPS AKA is performed when the user attaches to EPS via E-UTRAN access. Once the MME knows the user's IMSI, the MME can request an EPS authentication vector (AV) from the HSS/AuC as shown in Fig.2. Based on the IMSI, the HSS/AuC looks up the key K and a sequence number (SQN) associated with that IMSI. The AuC steps (i.e. increases) the SQN and generates a random challenge (RAND). Taking these parameters and the master key K as input to cryptographic functions, the HSS/AuC generates the UMTS AV. This AV consists of five parameters: an expected result (XRES), a network authentication token (AUTN), two keys (CK and IK), as well as the RAND.

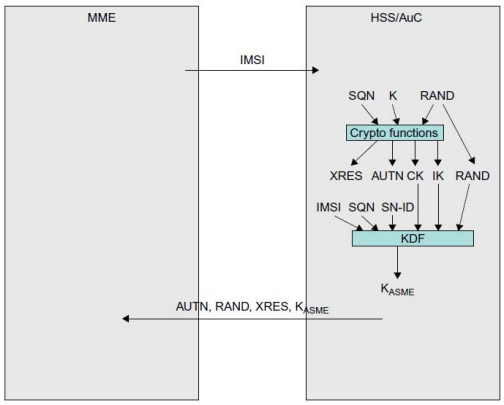


Fig.2. MME fetching the EPS Authentication Vector from Hss/AuC [10]

For E-UTRAN, however, the CK and IK are not sent to the MME. Instead the HSS/AuC generates a new key, KASME, based on the CK and IK and other parameters such as the serving network identity (SN ID). The SN ID includes the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the serving network. A reason for including SN ID is to provide a better key separation between different serving networks to ensure that a key derived for one serving network cannot be used in a different serving network. Mutual authentication in E-UTRAN is performed using the parameters RAND, AUTN and XRES. The MME keeps the KASME and XRES but forwards RAND and AUTN to the terminal shown in Fig.3.

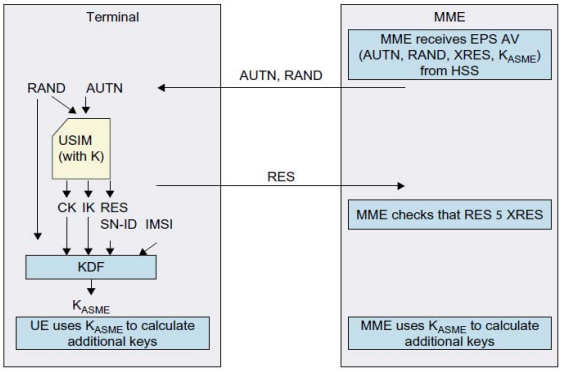


Fig.3. EPS AKA between UE and MME [10]

Both RAND and AUTN are sent to the USIM. AUTN is a parameter calculated by the HSS/AuC based on the secret key K and the SQN. The USIM now calculates its own version of AUTN using its own key K and SQN and compares it with the AUTN received from the MME. If they are consistent, the USIM has authenticated the network. Then the USIM calculates a response RES using cryptographic functions with the key K and the challenge RAND as input parameters. The USIM also computes CK and IK in the same way as when UTRAN is used (it is after all a regular UMTS SIM card). When the terminal receives RES, CK and IK from the USIM, it sends the RES back to the MME. MME authenticates the terminal by verifying that the RES is equal to XRES. This completes the mutual authentication.

The UE then uses the CK and IK to compute KASME in the same way as HSS/AuC did. If everything has worked out, the UE and network has authenticated each other and both UE and MME now have the same key KASME. (Note that none of the keys K, CK, IK or KASME was ever sent between UE and network [4].

Once the keys have been established in the UE and the network it is possible to start ciphering and integrity protection of the signalling and user data. The standard allows use of different cryptographic algorithms for this and the UE and the NW need to agree on which algorithm to use for a particular connection. For more details on which ciphering and integrity algorithms are supported with E-UTRAN, please see 3GPP TS 33.401 [10, 11].

As illustrated in Fig.2 and Fig.3, LTE authentication procedure works as follows:

1) MS sends international mobile subscriber identity (IMSI) and authentication request to (MME) (Mobility Management Entity).

2) MME passes this authentication request to HSS.

3) HSS, first verifies IMSI and SNID, then generates authentication vectors AV (1 . . . n) and sends the authentication data response AV (1 . . . n) to MME. This AV consists of: the random number, KASME, XRES and authentication token (AUTN). The authentication vectors are ordered by the sequence number.

4) MME stores authentication vectors, selects authentication vector AV (i), and sends authentication request (RAND (i), AUTN (i)) to MS. In the MME based on timer for validation KASME key, each authentication vector used for some authentication events. This means that full authentication procedure is not needed for every authentication event.

5) MS computes and retrieves the following parameters:
XAK=f5k (RAND), SQN=XAK⊕ SQN⊕AK,
XMAC=f1k (SQN ‖ RAND ‖ AMF) =? MAC, XSQN=?
SQN, RES=f2k (RAND)

(6) MME compares the received RES with XRES. If they match, then authentication is successfully completed. Next MME &MS retrieves KASME and agree with each other and, MS andMME use KASME for retrieving other all integrity and ciphering key according to Fig2 and starts security mode command procedure (SMC).All five messages has been shown in Fig4.

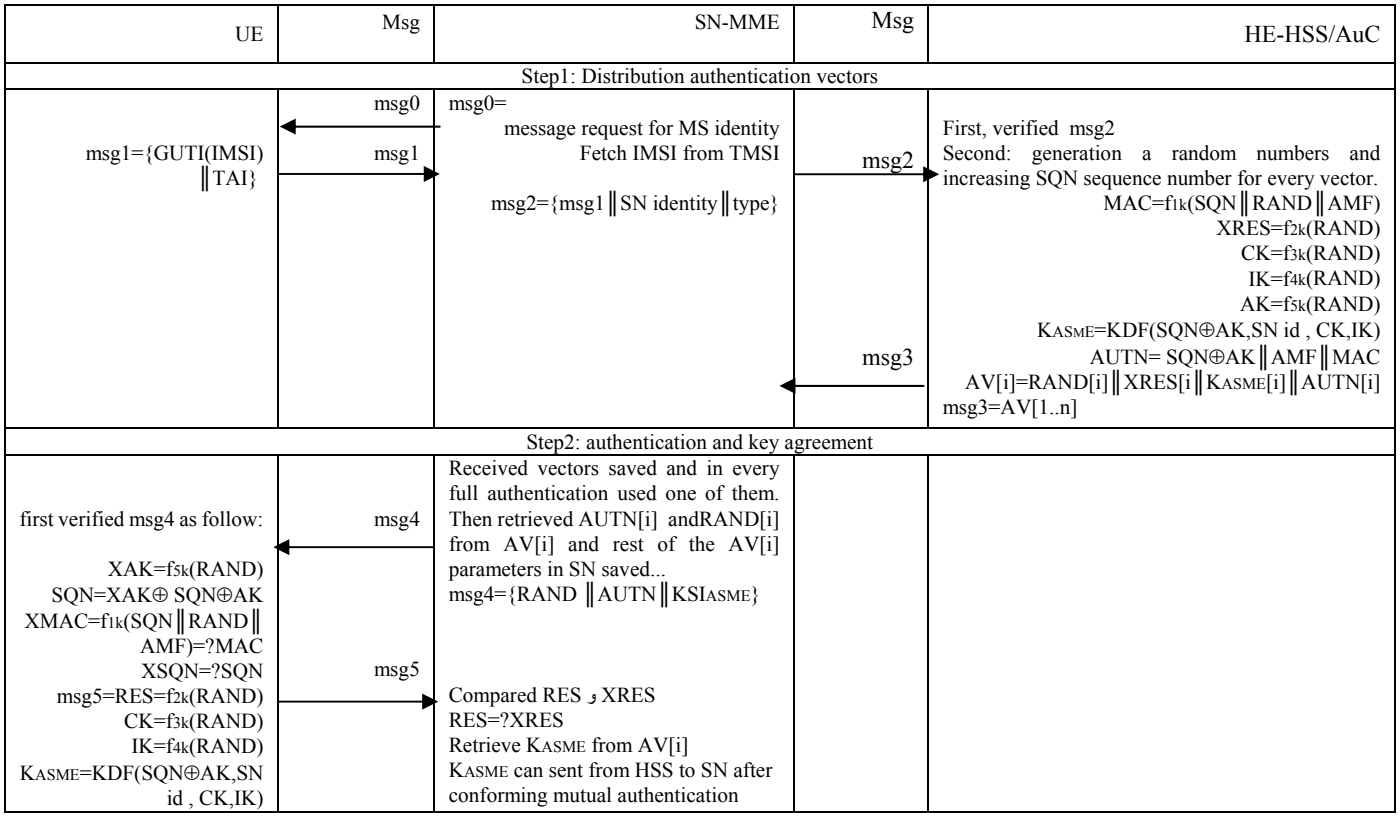


Fig. 4. EPS-AKA procedure

III. Improved Proposed-Aka Mechanism And Its Analysis Compared To EPS-Aka

The cryptographic algorithms f1, and f2, and the four key generation functions f3, f4, and f5 are shared between MS, SN and the HE. The secret key K is also share between MS and HE. The proposed protocol here works in two steps (A, B) as follows:

A. the goal for this steps is generation one authentication vector by HSS and send it to MME, so three messages should be transact between MS,MME, and HSS :

msg1: MS generate random number (MSR), MSMAC=f_{1K} (MSR) and sends msg1= {GUTI (IMSI (‖TAI‖MSR‖ MSMAC} to MME. then, during msg2 andmsg3, MS can calculate these parameters: MSCK=f_{3k} (MSR), MSIK=f_{4k} (MSR) MSRES=f_{2k} (MSR), MSAK=f_{5k} (MSR) so it doesn't cause delay.

msg2: in MME m random numbers as m random keys are generated and for every random key, n random numbersare generated in ascending order and the least NO used in every full authentication procedure as freshness assurance and to avoid replay attack .

RES *[i,j]*=f2SNR[i](RAND*[i,j]*),
CK *[i,j]*=$f_{3SNR[i]}$(RAND*[i,j])*,
IK *[i,j]*=$f_{4SNR[i]}$(RAND[*i,j]*),
KASME[*i,j*]=KDF(SNR[*i*],SN id , CK[*i,j],IK[i,j]),*
SNAV*[i,j]*=(RAND[i,j]‖RES[i,j]‖ KASME[i,j]), (i and j , in order is 0…m and 0…n),
msg2= {msg1‖SN identity‖type‖SNR[i]} is sent to HSS.

msg3: In HSS after verification msg2 and retrieving random key (SN[i]) andrandom number (MSR), parameters for one vector is calculated as follows:

HEMAC[i] =f_{1k} ((MSR⊕SNR[i]) ‖AMF)
HEAK=f_{5k} (MSR),
HECK=f_{3k} (MSR),
HEIK=f_{4k} (MSR),
HERES=f_{2k} (MSR),
HEAUTN[i] = (HEAK⊕ SNR[i] ‖AMF‖HEMAC[i])
HEKASME[i] =KDF (HEAK⊕ SNR[i], SD id, HECK, HEIK), msg3=HEAV[i] = (HEAUTN[i], HERES, HEKASME[i])

The authorized times of using the same SNR can be recognized by HSS.

msg 3 as a HEAV is sent to MME and the second step (B) is performed:

B. authentication and key agreement

msg4: in MME, n set random number (RAND [i,j]) related to random key which sent to HSS (SNR[i]) is retrieved and two parameters as follows is calculated:
MAC=$f_{1SNR[i]}$ (HEMAC[i], RAND [i,j]) ,
AUTN= (HEAK ⊕ SNR[i], AMF, MAC) and
msg4=RAND [i,j] ‖AUTN‖KSIASME, sent to MS.
KSIASME is 3 bits which is an index for validation KASME.

msg 5: in MS to avoid replay attacks , RAND[i,j] compared with last saved random number, if it is in correct rang then, checks the number of used same SNR, if it is more than authorized limit, authentication rejected. If it does not so, fallowing parameters calculated:
XSNR[i] = (HEAK ⊕ SNR[i]) ⊕ MSAK,
XHEMAC=f_{1k} ((MSR ⊕XSNR[i]) ‖AMF),
XMAC=f_{1XSNR} (XHEMAC, RAND [i,j])=?MAC,
if these equivalent is correct MS authenticates network and sends msg5=XRES=f_{2XSNR}(RAND[i,j])⊕ MSRES to MME, in MME if RES=RES[i,j] ⊕ HERES[i]=?XRES is correct, MME authenticate MS and authentication will be

successful. Next MME andMS agree on integrity and ciphering keys with each other as follows:

In MS: XCK [i,j]=$f3_{XSNR[i]}$(RAND[i,j]) ,

XIK [i,j]=$f4_{XSNR[i]}$(RAND[i,j]) ,

MSK_{ASME}[i] =KDF (MSAK ⊕ XSNR[i], SN id, MSCK, MSIK),

K_{ASME}[i,j]=KDF(XSNR[i],SN id , XCK[i,j],XIK[i,j]),

K_{ASME}= K_{ASME} [i,j] ⊕ MSK_{ASME}[i]

In MME: K_{ASME}= K_{ASME} [i,j] ⊕ HEK_{ASME}[i]

All five messages have been shown in Fig.5 and Fig.6.

In this section both EPS-AKA and proposed-AKA from the viewpoint of bandwidth consumption between SN and HE and computation overhead in HE are compared. Note that, the analysis is based on vector based-AKA, not key reuse based-AKA. Assume the topology of cellular network, according to Fig7, every cell covered by one eNodeB, every 7 eNodeB is specified boundary of one TA and one MME covered 21 eNodeBs or tree TA.

The mobile station is continuously listening to the broadcast message from MME to identify the Tracking area by using tracking area identity (TAI); the MS is comparing the TAI which is received with the TAI stored in the USIM. When the TAI is different, the MS requires a new TAU. Registration occurs when the mobile is switched on, or when it has moved from one registration area to a new one. Movement of MS within the same registration area will not generate any registration messages. The authentication processes is done in every TAU, registration, call originating, call terminating, and handovers.

In this model, we have the following parameters:

1) User who is carrying mobile station (MS) is moving at an average velocity v;

2) Direction of MS movement is uniformly distributed over [0, 2π];

3) Mobile users are uniformly populated with the density within the area;

4) One eNB area boundary is length of L1, Tracking Area (TA) boundary length of L2 and, MME area boundary is length of L3.

The average number of active mobile crossing the area boundary of length L, is given by [12]

$$R= (\rho.\nu .L)/\pi. \quad (1)$$

From (1), we can calculate the signaling traffic for every authentication events in LTE network including: origination, termination call, handovers, Registration and TAU (Tracking Area Update).

Note that handover happen when MS is in active mode and is moving from one cell to another cell, TAU happen when MS is in idle mode and moving from one TA to another TA and Registration happen when MS is switched on or moved from one SN to other SN.

The traffic due to authentication request of handover is generated by mobile moving into new cell:

R (handover, eNB) = (ρ1.ν .L1)/π

R (handover, MME) = R (handover, eNB) × Total number of eNB area in one MME area

R (handover, HSS) = R (handover, eNB) × Total number of eNB area in one HSS area

The traffic due to authentication request of TAU is generated by mobile moving into new tracking area:

R (TAU, TA) = (ρ2.ν .L2)/π

R (TAU, MME) = R (TAU, TA)× Total number of TA in one MME area

R (TAU, HSS) = R (TAU, TA)× Total number of TA in one HSS area

The average originating and terminating service requests rate

R (service request/HSS) = average service origination rate× total of MS,

R (service request/MME) = R service request/HSS/number of MME area in HSS area,

The number of service requests terminating per HSS or MME area (R (service request/HSS), R (service request/MME)) is equivalent to the number of service requests originating per HSS or MME area.

If, P1 is being probability of requests which need to access HSS and P2 is the probability of requests which doesn't need to access HSS and n is the number of vectors in every access to HSS for every MS, so we will have:

$$P1=1/n \quad , \quad P2= (n-1)/n$$

MS	msg	SN-MME	msg	HE-HSS/AuC
Step1: Distribution authentication vectors				
MSMAC=f1k(MSR)	**msg0**	msg0= message request for MS identity		
msg1={GUTI(IMSI) ‖ TAI ‖ MSR ‖ MSMAC }	**msg1**	RES[i,j]=f2SNR[i](RAND[i,j])		First, verified msg2 Second: derived MSR and SNR then, computed XMSMAC by MSR. **XMSMAC= f1k(MSR)=?MSMAC**
		CK[i,j]=f3SNR[i] (RAND[i,j])	**msg2**	HEAV[i] is computed as follows:
		IK[i,j]=f4SNR[i] (RAND[i,j])		HEMAC[i]=f1k((MSR,SNR[i]),AMF)
MSCK=f3k(MSR)		KASME[i,j]=KDF(SNR[i],SN id , CK[i,j],IK[i,j])	**msg3**	HEAK=f5k(MSR) HECK=f3k(MSR)
MSIK=f4k(MSR)		SNAV[i,j]=(RAND[i,j] ‖ RES[i,j] ‖ KASME[i,j])		HEIK=f4k(MSR) HERES=f2k(MSR)
MSRES=f2k(MSR)				HEAUTN[i]=(HEAK⊕ SNR[i] ‖ AMF ‖ HEMAC[i])
MSAK=f5k(MSR)		msg2={msg1 ‖ SN id ‖ type ‖ SNR[i]}		HEKASME[i]=KDF(HEAK⊕ SNR[i],SD id, HECK,HEIK) msg3=HEAV[i]=(HEAUTN[i],HERES, HEKASME[i]) HEAV[i] is the only vector that transfer to SN

Fig. 5. Step1 of proposed AKA protocol: Distribution authentication vectors

MS	msg	SN-MME	msg	HE-HSS/AuC
Step2: authentication and key agreement				
First: compared the new RAND[i,j] and the old RAND[i, j] XSNR[i]=(HEAK ⊕ SNR[i]) ⊕ MSAK Then the following parameter is computed: XHEMAC=f1k((MSR ⊕XSNR[i)‖AMF) XMAC=f1XSNR(XHEMAC,RAND[i,j])=?MAC msg5=XRES=f2XSNR(RAND[i,j])⊕ MSRES XCK[i,j]=f3XSNR[i] (RAND[i,j]) XIK[i,j]=f4XSNR[i] (RAND[i,j]) MSKASME[i]=KDF(MSAK ⊕ XSNR[i],SN id , MSCK, MSIK) KASME[i,j]=KDF(XSNR[i],SN id , XCK[i,j],XIK[i,j]) KASME= KASME[i,j] ⊕ MSKASME[i]	**msg4** ← **msg5** →	First : derived RAND[i,j] ، CK[i,j] ، IK[i,j] related to SNR[i], then from received vector(HEAV[i]), derived HEAUTN[i] and HEMAC After that the follows parameter is driven. MAC=f1SNR[i] (HEMAC[i], RAND[i,j]) AUTN=(HEAK ⊕ SNR[i], AMF, MAC) msg4=RAND[i,j] ‖AUTN‖KSIASME RES=RES[i,j] ⊕ HERES[i]=?XRES KASME[i,j] , related to SNR[i], by CK[i,j] ، IK[i,j] is driven. KASME= KASME[i,j] ⊕ HEKASME[i]		

Fig. 6.Step2 of proposed AKA protocol: authentication and key agreement

The length of authentication parameters (bits) is as follows [11]:

- AMF,SQN,AK =48 bits
- RES,MAC,Type,TAI =64 bits
- KSIASME=3 bits
- AUTN=160 bits(EPS-AKA) and HEAUTN =240bits(proposed-AKA)
- AV=608 bits (EPS-AKA) and AV=560 bits (proposed-AKA)
- Service request=8 bits

In proposed-AKA, k is the number of random number related to each random key (SNR) of MME.

Above length authentication parameters enable us to compute the bandwidth consumption for each activity by MME and HSS. The size of messages between all nodes evolved in authentication procedure (MS, MME, and HSS) and communication overhead of that, in both proposed-AKA and EPS-AKA can be calculated as follows:

(EPS-AKA, MME):

((n-1)/n × number of bits
+ 1/n× number of bits)×(average number of authentication events per MME)
= ((n-1)/n× (L (msg1)
+L (msg4) +L (msg5))
+ 1/n× (L (msg1) +L (msg2) +L (msg3) +L (msg4)
+ L (msg5)))×(average number of authentication events per MME)
= ((n-1)/n× (L ({GUTI (IMSI) ‖TAI})

+L ({RAND ‖AUTN‖KSIASME}) +L (RES))

+ 1/n×(L ({GUTI (IMSI) ‖TAI})

+L ({msg1‖SN identity‖type}) +L (AV [1...n])

+L ({RAND ‖AUTN‖KSIASME}) + L (RES)))×(average number of authentication events per MME)

= (n-1)/n × (192+291+64)
+ 1/n× (192+448+608×n+291+64))
×(average number of authentication events per MME)

(Proposed-AKA, MME):

((k-1)/k × number of bits+ 1/k× number of bits)×(average number of authentication events per MME)

= ((k-1)/k× (L (msg1)

+L (msg4) +L (msg5))

+ 1/k× (L (msg1) +L (msg2) +L (msg3) +L (msg4) + L (msg5)))×(average number of authentication events per MME)

= ((k-1)/k× (L ({GUTI (IMSI‖ (TAI‖MSR‖ MSMAC})

+L (RAND [i,j] ‖AUTN‖KSIASME)+L(XRES))

+ 1/k× (L({GUTI (IMSI‖ (TAI‖MSR‖ MSMAC })

+L ({msg1‖SN identity‖type‖SNR[i]})

+L (HEAV[i]) +L (RAND [i,j] ‖AUTN‖KSIASME)

+ L (XRES)))×(average number of authentication events per MME)

= ((k-1)/k × (320+371+64)
+ 1/k× (320+640+560+371+64))×(average number of authentication events per MME)

(EPS-AKA, HSS):

1/n×2× (L (msg2)
+L (msg3))×(average number of authentication events per HSS)

=1/n×2× (L ({msg1‖SN identity ‖type})
+L (AV [1...n]))×(average number of authentication events per HSS)

= 1395.2×(average number of authentication events per HSS)

(Proposed –AKA, HSS):

1/k×2 (L (msg2)

+L (msg3))×(average number of authentication events per HSS)

=1/k×2× ((L ({msg1‖SN identity‖type‖SNR[i]}) +L (HEAV[i])) ×(average number of authentication events per HSS)) ×(average number of authentication events per HSS)

= 480×(average number of authentication events per HSS).

IV. Simulation Results

According to the topology of Fig7, Simulation study and implementation on the software, has been carried out in order to analyze signaling traffic performance, load transaction messages and bandwidth consumption that is consumed between mobile networks entities. The software we have used to simulate the current and proposed authentication protocol is MATLAB R2009a.

In both proposed-AKA and EPS-AKA protocols, the number of signaling messages between the mobile networks entities are the same and it is 5 messages. The simulation results show that the load transaction messages, bandwidth, number of computed hash function (f andKDF) between entities comparing to current protocol are minimized, as

Illustrated in Fig. 4, 5, and 6. Therefore, the performances of authentication have been improved significantly.

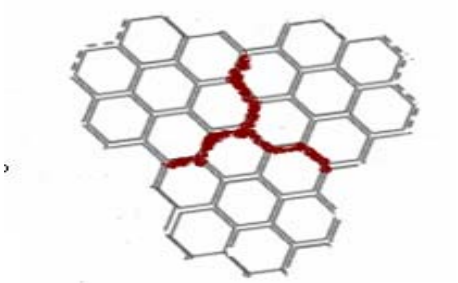


Fig.7. 21 Cells which is equivalent to 21 eNBs area definition

It is clear that, in EPS-AKA, bandwidth consumption depends on access times to HSS and the number of computed vectors in every access to HSS, whereas, in proposed –AKA bandwidth consumption just depend on access times to HSS, because, in each access time to HSS just one vector is requested by MME. So as illustrated in Fig8 (a), except n=1, bandwidth consumption by HSS in proposed-AKA is always lower and by increasing mean density of MS.

Fig.8.(a) illustrates bandwidth consumption of exchanged messages between HSS and MME in both new proposed AKA protocol and standard EPS-AKA protocol under the same traffic conditions with different number of authentication vectors in each access times of MME to HSS (n) in two different average density of MS.

The curves in Fig.8. (a) shows that bandwidth consumption in the new proposed protocol in all n except n =1, always is less than the standard EPS-AKA protocol and with increasing n the bandwidth consumed in the new proposed AKA protocol due to less access to HE, always has a downside, while bandwidth consumption in the standard EPS-AKA protocol has decreasing trend, up to n=6 and in more than n=6 being fix and equal 5.5MB/Ses. Also, the average density of MS with 10 times more (30/km^2 to 300/km^2), the average number of authentication events, including the number HO, location update (TAU) and the service requests, are increased. Therefore the avg. number of authentication events as well as bandwidth consumption between SN and HE will be increased.

If by the above reasons, the amount of authentication events is been very high, authentication signalling traffic overhead will be increased remarkably, especially, because of substantial changes in the structure cellular networks and integrated core network, this problem will be in Next Generation mobile Networks much greater.

Table 1 shows the basic assumptions of parameters. In the following two protocols has been compared by this table. The topology of cellular network which is assumed is like Fig7. As seen in Fig 7, is, each cell covered by one eNB, a 7 eNB (cell) covered by a TA, every 3 TA covered by one MME and also every 50 MME covered by one HE or HSS / AuC.

In Fig.8.(a) as the example in n = 5, with average density of MS equal to 300 ms/km^2, the bandwidth consumption in the new proposed protocol compared to standard protocols almost 65% is being reduced while at the same n and the density 30 ms/km^2 , bandwidth consumption in new proposed protocol compared to standard protocol has been reduced less than 10%, this is because of two reasons , bandwidth consumption is affected first by increasing number of access to the HSS and for the second, increasing the number of vectors which are calculated in each access times to HSS (n).

According to the mechanism defined by the new proposed protocol, increasing n has no effect on bandwidth consumption, because in each access to the HSS in a new protocol n is equal to 1.

TABLE1: Assumption Parameter

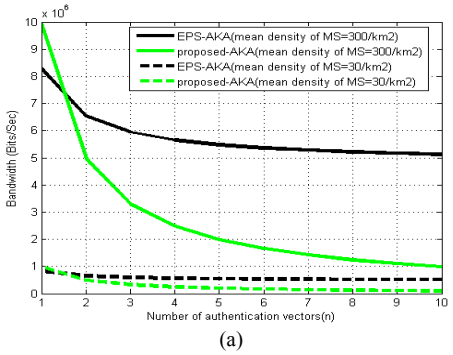
Covered area by HSS	
parameters	quantities
Number of eNodeB	1050
Number of TA	150
Number of MME	50
(ρ1) Mean density of active MS	300/km2
(ρ2) Mean density of idle MS	300/km2
(Switch on MS)Number of active and idle MS	1635000
Avg. rate of originating service request	3.2/hr/user
Avg. rate of terminating service request	3.2/hr/user
(L1) Border covered by eNodeB	6 km
(L2) Border of TA	18 km
(L3) Border covered by MME	36 km
area covered by eNodeB	2.6 km2
area of TA	18.2km2
area covered by MME	54.5 km2
(ν) Avg. Velocity of MS	4.3 km/hr

In new proposed protocol when traffic volume is being increased in HSS, can be increased n, for reducing access to HSS , while in the standard protocol , n can increase to some extend, for example after n =6 bandwidth consumption about to be constant , but in the new protocol, bandwidth consumption not only reduces but also computation in HSS is constant.

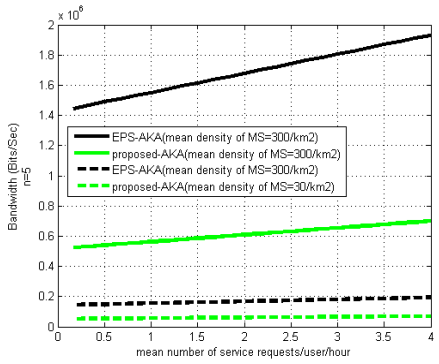
Thus, bandwidth consumption in the proposed protocol always smaller than the EPS-AKA protocol, and when the average density of MS being ten times more, the difference authentication of communication traffic overhead being more considerably.

In fact the original target of this new proposed authentication protocol is its application to reduce bandwidth consumption substantially, when the number of authentication events is high and network is being busy, which lead to a significant decreasing of bandwidth consumption by reducing messages exchanged between HSS and MME.

As illustrated Fig.8 (b), at the same traffic conditions and respect to five vectors in each access times to the HSS (n equal to 5), when the average rate of service requests/MS/hour is being increased, firstly bandwidth consumption in new proposed protocol always is less than standard EPS-AKA and secondly the reducing steep in proposed protocol is less than other one. Also, in the average mobile density/km^2 equal to 30, both protocol almost have the same bandwidth consumption, while in 10 times more (300MS/km^2), the difference of bandwidth consumption for both protocols is being more considerable.



(a)



(b)

Fig. 8.Bandwidth consumption by HSS in both EPS-AKA and proposed AKA (a and b)

To compare the cost of computation overhead, the number of computed security functions in both protocols of LTE network during execution of AKA protocol is considered. Although the various security functions in the process authentication protocol have different calculations overhead, for comfort the calculation overhead costs, with respect to the structure of the core algorithms used in all authentication functions and key production function, are the same (SHA: Secure Hash Algorithm[13,14]), we assume the same weight of calculation cost for all function.

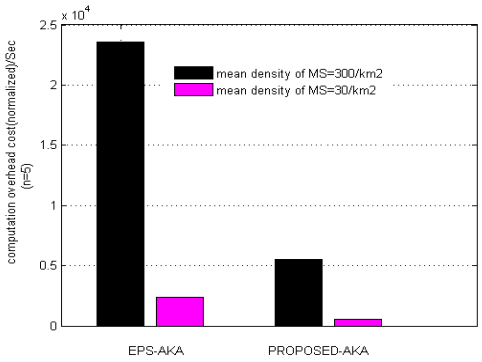


Fig. 9. Computation overhead cost in both EPS-AKA and PROPOSED-AKA

It should be notice that all computation SN in the first step of proposed AKA protocol can calculate before and reuse for the different MS, but not at the same time and same parameter for the different MS.

The bar plot Fig.9, shows the comparison of computation overhead cost of both new and standard authentication protocol in HSS. We assume the number of vectors in every access to HSS is n=5. As you see, the computation overhead cost of new proposed protocol compared to standard one in lower and the difference between them by increasing mean density of MS is being considerable. So by increasing number of MS, superior new proposed protocol is clear.

I. Conclusion

because of provision of different type of services and integration Next Generation mobile Networks (LTE and 4G) and create secure channels between all elements in the network, in addition to the service requested and tracking area updates as an authentication trigger, different types of HO (handover) is added, therefore this issue, causes to increase authentication traffic overhead and the signalling costs. This paper has pointed to resolved and unresolved security and traffic issues for 3GPP SAE AKA and in section III to improve performance of authentication protocol originality in the LTE network and better management the authentication signalling traffic overhead, a new proposed authentication protocol is suggested to resolve some defects, such as AKA computation in HSS and bandwidth consumption. In fact, Analysis shows that the performance of standard EPS-AKA protocol in the LTE network is improved by new proposed protocol which made lower bandwidth consumption and calculation during execution of AKA protocol.

The result in this paper proposes the necessity in studying security management, and signalling traffic overhead together. Investigating the authentication traffic

characteristics in the future heterogeneous networks is also an interesting problem.

REFERENCES

[1] Z. Y. Shi, Z. Ji, Z. Gao and L. Huang, "*Layered Security Approach in LTE and Simulation"* Department of EED Xiamen University, Xiamen,Fujian,China.

[2] Yi-Bing Lin and Yuan-Kai Chen, "Reducing authentication signaling traffic in *third*-Generation mobile network," *IEEE Transactions on Wireless Communications*, Vol.2, No.3, May 2003.

[3] J. Al-Saraireh and S. Yousef, "Analytical model for *authentication* transmission overhead between entities in mobile networks," *Elsevier Computer Communications*, Vol.30, 8, June 2007.

[4] Y. Zhang and M. Fujise, "An improvement for authentication protocol in third-generation wireless networks," *IEEE Transactions on Wireless Communications*, Vol.5, No.9, September 2006.

[5] Lin-Yi Wu and Yi-Bing Lin, "Authentication vector management for UMTS*," IEEE Transactions on Wireless Communications*, Vol.6, No.11, November 2007.

[6] C. Huang and J. Li, "Authentication and key agreement protocol for UMTS with low bandwidth consumption*,"* in *Proc. of the 19th International Conference on Advanced Information Networking and Applications (AINA),* March 2005.

[7] J. Al-Saraireh and S. Yousef*, "A new authentication protocol for UMTS mobile networks," EURASIP Journal on Wireless Communications and Networking*, Vol.2006, Issue 2, April 2006.

[8] 3GPP TS 33.060," General Packet Radio Services (GPRS)"; Service description, *stage* 2.

[9] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A *Tutorial*," *IEEE Communications Magazine*, February 2009.

[10] M. Olsson, S. S. S. Rommer, L. Frid, C. Mulligan "SAE and the Evolved Packet Core: Driving The Mobile Broadband Revolution'' Academic Press, First edition 2009.

[11] Third Generation Partnership Project; Technical Specification Group Services *and* System Aspects; 3GPP System Architecture Evolution (SAE), "Security Architecture Security (Release 8)," 3GPP TS 33.401 version 8.2.1, December 2008

[12] G. P. P. Kathleen. Meier-Hellstern and David 1. Goodman''Signaling Traffic Volume Generated by Mobile and Personal *Communications''IEEE* Communications Magazine June 1995.

[13] *XSmart e-Passport V1.1 Security Target, Document ID: XSMART_ASE_LITE, Copyright 2010 – LG CNS Co., Ltd. All rights reserved.*

[14] *3GPP2 S.S0055-A, "Enhanced Cryptographic Algorithm" 26 September 2005*