International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, Number 20 (2017) pp. 9306-9314
© Research India Publications. http://www.ripublication.com

Reducing Authentication Signaling Traffic for LTE Mobile Networks

Ja'afer Al-Saraireh

Computer Science Department, Princess Sumaya University for Technology,
Amman 11941, Jordan.
Orcid: 0000-0001-9424-9496

Abstract

With the spread of many smartphones, LTE network has provided various and fast mobile services. Many mobile devices use more wireless services than ever before, therefore; lot of authentication signaling is required. Authentication in such a wireless network plays an important role in identifying a wireless device and is also the beginning of a wireless network. Therefore, in this paper, we analyze the pattern of authentication that occurred before devices accessing the network.

Therefore, this research proposes a fast wireless authentication service by minimizing the signaling traffic cost between the mobile network entities for LTE. The rate at which authentication occurs in the LTE network was calculated using mathematical modeling, and the change in the cost of authentication signaling in various environments was calculated. In this paper, we show that the number of optimal authentication data is calculated and the cost of authentication signaling is more efficient than before.

Keywords: LTE; EPS; EPC; E-UTRAN; Authentication Vector; and Residence Time.

Abbreviation

ADR	Authentication Data Response
AK	Anonymity Key
AMF	Authentication Management Field
APN	Access Point Name
AUTN	Authentication Token
AV	Authentication Vectors
CK	Cipher key
eNB	Evolved base stations
EPC	Evolved Packet Core
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network
HSS	Home Subscriber Server
IK	Integrity Key
IMSI	International Mobile Subscriber Identity
KDF	Key Derivation Function
LTE	Long Term Evaluation
MAC	Message Authentication Code
MME	Mobility Management Entity
MT	Mobile Terminal
P-GW	Packet data Network Gateway
RAND	Random number
S-GW	Serving Gateway
SNID	Serving Network Identity
SQN	Sequence Number
TA	Tracking Area
TAU	Tracking Area Update
TE	Terminal Equipment
TMP	Trusted Mobile Platform
UAR	User Authentication Request
UE	User Equipment
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
WPKI	Wireless Public-Key Infrastructure
XRES	Expected Response

INTRODUCTION

The LTE is one of the 4G mobile broadband. The architecture of LTE network was presented in figure 1. LTE includes three components are: UE, E-UTRAN and the EPC [1]. The UE for LTE is included MT, TE and UICC. The MT to manage the communication function, TE to terminate the data streams, and UICC which identified as the SIM card [2]. The USIM is an

application runs by the SIM. The SIM card includes user's phone number, home network identity and security keys etc. The radio communication between mobile networks are handled by E-UTRAN. The eNB is has one component of E-UTRAN.

The EPC has the following components: HSS, P-GW, S-GW and MME. HSS is a centralized database for the subscriber's information. The P-GW is employed to communicate the outside world i.e. PDN by using SGi user interface. Each PDN is known by an APN. The S-GW acts as router to forward data between base station and P-GW. The MME controls the high level operation of the mobile by means of signaling messages and HSS [1].

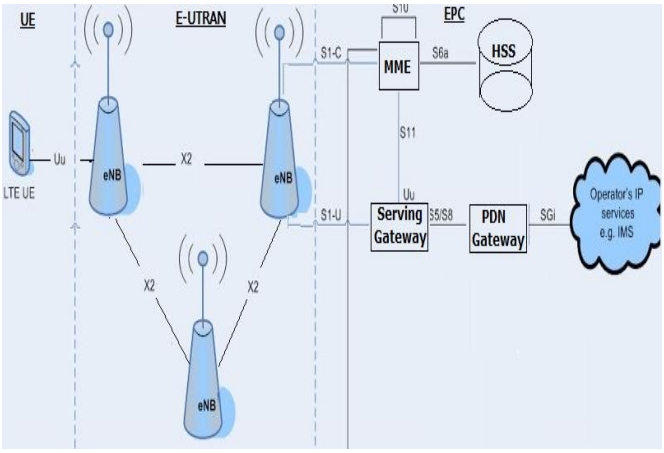

Figure 1: Architecture of LTE Network

The paper is structured as follows: next section describes the LTE authentication and key management process. The related works are presented in this research. The proposed approach is presented in the section of proposed approach for dynamic length for authentication vector. The mathematical model for proposed approach is presented in modeling analysis section. Th performance analysis and discussion results are presented in this research. The paper is concluded in final section.

LTE AUTHENTICATION PROCEDURE AND KEY MANAGEMENT PROCESS

An authentication process is used to allow all subscriber's to show their authority and validate the user's identities [3]. This process using UE secret key *K*, RAND, crypto functions - include f_1, and f_2 which are message authentication code functions and f_3, f_4, f_5 and *KDF* which are key generation functions. KDF that are shared between UE and the HSS [3] [4]. The HSS retains a SQN_{HSS}, where UE retains SQN_{UE}.

A mutual authentication between UE, MME and HSS is carried away when the UE moves from one communication area to another, the AV is generated at HSS and sent to UE by MME. Figure 2 and 3 describes LTE authentication and key management process as follow:

1. When UE enters to a new the communication area of eNB then attach request sends by UE to MME. This attach request contains IMSI, UE security capability, and Key Security Identifier (K_{ASME})
2. MME delivers ADR to HSS, ADR includes IMSI, SNID, and network type (wire/wireless).
3. HSS authenticate SNID when HSS acquiring ADR from MME. If the HSS authenticated SN successful, then HSS restive the UE secrete key (K_{UE}) from it database.
4. Authentication vectors is created by HSS and then the MME received the ADR from HSS, where each AV contains of four components: AUTN, RAND, XRES and K_{ASME}. The AV is generated as follow [3][5][6]:
   - **i.** HSS generates SQN_{HSS} and RAND.
   - **ii.** HSS computes the following
     a. $CK = f_3(K_{UE}, RAND)$.
     b. $AK = f_5(K_{UE}, RAND)$.
     c. $IK = f_4(K_{UE}, RAND)$.
     d. $XRES = f_2(K_{UE}, RAND)$.
     e. $K_{ASME} = KDF(SQN \oplus AK, CK||IK||SNID)$.
     f. $MAC = f_1(K_{UE}, SQN||RAND||AMF)$.
     g. $AUTN = (SQN \oplus AK||AMF||MAC)$.
     h. $AV = RAND \,||\, XRES \,||\, AUTN||\, K_{ASME}$.
   - **iii.** HSS increments SQN_{HSS} by 1.
5. HSS sends ADR to MME, the ADR containing AVs.
6. AV is stored in MME, then MME chooses the i^{th} AV(i). MME generates and sends a UAR to UE, the UAR contains RAND(i), AUTN(i), and K_{ASME}.
7. UE receives UAR from MME and then UE calculates the following:
   - **i.** $AK = f_5(K_{UE}, RAND)$.
   - **ii.** $SQN = ((SQN \oplus AK) \oplus AK)$.
   - **iii.** $XMAC = f_1(K_{UE}, SQN||RAND||AMF)$.
   - **iv.** MAX which is contained within AUTN is matched with XMAC. If the comparison failed, then UE generates and sends error message to MME. Otherwise; UE validates the SQN which received is in the accurate range. (i.e. $SQN > SQN_{UE}$). If the comparison failed then UE generates and sends error message to MME. Otherwise; UE generates RES, CK, IK, K_{ASME} as following: RES =

$f_2(K_{UE}, RAND)$, $CK = f_3(K_{UE}, RAND)$, $IK = f_4(K_{UE}, RAND)$, and $K_{ASME} = KDF(SQN \oplus AK, CK||IK||SNID)$.

8. UE sends UAR which includes RES to MME
9. When MME receives the user authentication response, it matches the RES which received with XRES. If the matching successful, then a successful mutual authentication is achieved and the connection is established. Otherwise the authentication failed and reject the connection which requested by UE.

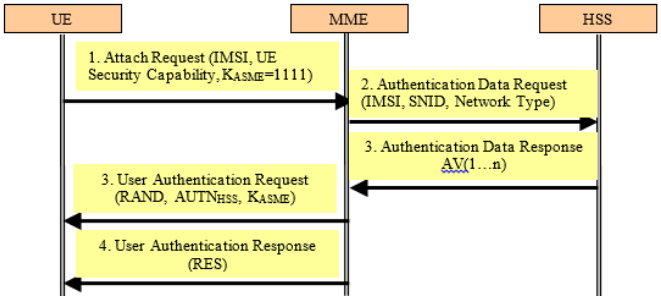

Figure 2: LTE Authentications

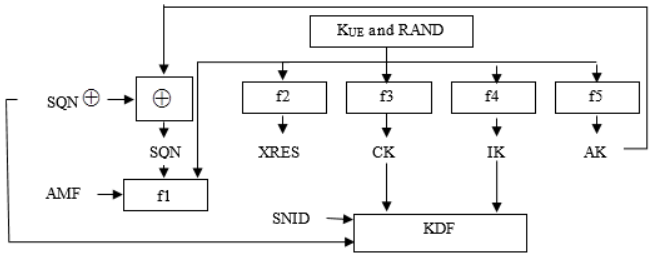

Figure 3: Generation of authentication vector

RELATED WORK

To improve the mobile network security, a several methods have been suggested. Many of studies have been focused on the AKA protocol. Some approaches adding new entities to manage authentication process by redesign the core network architecture.

There are no research studied the effect of the number of AV for LTE, while the effect of number of AV for AKA have been studied by [3][7][8][9].The pre-authentication approach has been proposed by Yan Zhang [8]. The authentication time was reduced by using pre-authentication approach, while the signaling overhead was increased[9].

A new scheme is proposed by [10] to avoid the network traffic and subsequent re-authentication delay. The standard EPS-AKA for LTE network has been studied by [11]. The proposed approach improves the performance of LTE network.

For 4G interoperability an EAP-AKA was suggested, a modification of the EAP-AKA specified by 3GPP was implemented that achieve security, the user identity was protected and the man-in-the-middle attack is avoided [12]. The proposed approach built on Elliptic Curve Diffie-Hellman.

J-PAKE mechanism was presented by [13] to improve the EPS-AKA security by presented perfect secret privacy property. Additionally, they spot a threat, absence of identification privacy, without mentioning any solution to grab it.

SE-EPS AKA was presented by [14] to protect the communications between all entities by using WPKI before the security framework is established [15]. The private should be stored in the USIM/MME/HSS in the proposed SE-EPS AKA. The main threats in SE-EPS approach are suffer from brute force and security of user identity is not provided by the suggested SE-EPS approach [16]. To overcome this problem, ECAKA was proposed by [16]. In the ECAKA public key protection mechanisms were used, the user identity and message integrity were protected by using encryption.

To perform mutual authentication among UE-MME-HSS, an EAKA approach was presented by [17]. The structure of AV and additional challenge parameter were used in this proposed approach. The proposed scheme assumes that the whole authentication process carried out by UE, without allocating any role in the mobile network entities. This technique needs more robust modifications of the current mobile system to be friendly with the re-defined USIM cards and AV.

A mobile network architecture improvement is suggested by [18][19]. The authors suggested to use biometric identity and TMP, then mutual authentication is achieved in a benign environment over the HAKA procedure. The solution based on local authentication for the UE and USIM, and remote authentication between UE and serving network. This method increases the traffic for authentication compared with AKA protocol and imposing the operators to attain biometric factors for each and every subscriber and store them on the main network.

A Y-Comm technique suggested by [20], this method deliver a solid system, where each level is protected enough to evade potential attacks. The proposed approach restructuring of the entire mobile system and increase cost and extra effort, making this solution is not acceptable for the operators.

An integration the International Mobile Station Equipment (IMEI) with the integrity key is suggested by [21]. The proposed mechanism reduced the bandwidth and the number of transactions for authentication by using Elgamal signature based authentication in LTE. This method called DS-AKA. The SGSN is authorized by HLR/AuC this leads to reduce the traffic between entities. The DS-AKA requires more time for authentication compared with 3GPP-AKA for initially authentication while the time is steady in the proposed protocol when the number of nodes in eNB is increased.

An integrating the LTE network into CNPC network was proposed by [22]. This approach requires an amendment to

AKA and handover key management protocol to remove vulnerabilities such as man-in-the-middle attack and eNB compromise attack. The communication overhead is still as same level as the LTE's protocols. The proposed approach requires six message to be exchange between the UE and network entities, and requires a UE to hold only a certificate for LTE authentication.

The AKA for interoperation between different mobile networks such as GSM, UMTS and LTE was studied by [23]. The authors found some attacks such as false base station attack which inherited from the GSM.

The strengths and deficiencies for LTE-Advanced was identified by [24]. The user location and man-in-middle arrack between UE and eNB occurs because the user identity transferred as clear text when an initial attached procedure compromised the entire system. The RRC signaling message is transferred as a clear text. Therefore; it is simply to sniffed and replied RRC signaling message to eNB several times to break down the system with traffic injection which lead to denial of service attack.

For update and to minimize the signaling load in the mobile networks, a study was carried out by [25][26] to explore how UEs determine for themselves an optimal input interval update and how the intervals used in key management process.

A new two techniques are proposed by [27] to minimize the initial authentication time. The first technique is called fast authentication, states data traffic temporarily through the network to the gateway and the immediate parent node of the joining node presents network-side authentication. The second technique is pre-fetch supported authentication, allows the authenticated wireless nodes to pre-fetch and store the authentication vectors of the prospective mobile clients. These schemes are well-suited for infrastructure-based multi-hop wireless communication because LTE required multiple rounds of message exchange between entities in multi hop infrastructure.

For handover update interval a framework for selecting an optimal key handover is proposed by[28]. The framework enables a network operator to select an optimal value fits best with network management policies.

Therefore; the efficiency for LTE networks in terms of traffic overhead and minimized the network traffic without damage to network security is needed.

PROPOSED APPROACH FOR DYNAMIC LENGTH FOR AUTHENTICATION VECTOR

In this research, a dynamic length for AV for LTE has been proposed to improve the performance of authentication process. This is accomplished by decreasing the signaling message traffic between LTE entities. The number of signaling transmission between LTE entities is minimized when the length of AVs is increased, While, when the length of AV is increased too large then the LTE network bandwidth is consumed for each signaling transmission between HSS and MME. It is a gentle to select appropriate length for AV to reduce the authentication signaling transmission cost and bandwidth consumption.

The HSS is responsible for generating AV and sends it to MME who is responsible for authenticated UE. The transmission cost is expensive between HSS and MME and the performance is down. Most of UEs are not consumed the AV which stored in MME.

The timing diagram for ADR and UAR is presented in Figure 4.

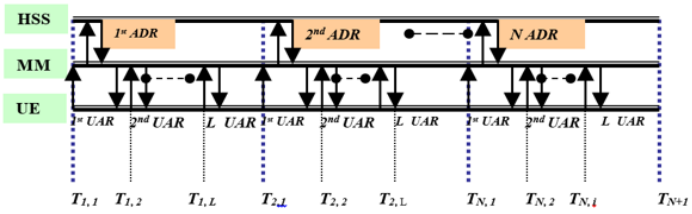

Figure 4: Timing Diagram

The UE resides from time $\mathcal{T}_{1,1}$to $\mathcal{T}_{\mathcal{N},1}$in the same tracking area TA, UE generates n ADR, AVs has $\mathcal{Q}$ records and at time$\mathcal{T}_{\mathcal{N},1}$, the UE leaves the TA. The last ADR is performed at time$T_{N,i}$, the MME uses only *i* records from last AV. The total number of UARs performed is $(n-1)*\mathcal{Q}+i$

Initially when UE sends attach request to HSS, the AV length assigned by default 5, but when UE generated 5 user authentication request the AV is consumed from MME, then MME sends a 2nd ADR to HSS then the length of AV *L(AV)* increment randomly by *i where* $1 \leq i \leq 5$. While UE resides in the same TA the $l(v)$ increment by *i*. At time $\mathcal{T}_{\mathcal{N}}$ the *L(AV)* is equal the length of AV at time $\mathcal{T}_{\mathcal{N}-1}+i$.

When UE move to new tracking area, the HSS is responsible to predict the length of AV based in the historical behavior for UE by using one of the following methods:

1. Using the average (AVM) to predicate the length of AV. The new $L(AV)=\left\lceil\frac{\#UARs}{\#ADRs}\right\rceil$. Based on the table 1, the total of ADRs = 11 and total UARs = 159. Then the new $L(AV)=\left\lceil\frac{159}{11}\right\rceil=15$.
2. Using Interquartile Range Method (IQRM) which is a measure if variability. This approach based on dividing a data set into quartiles. This technique is used to measure of the where the middle fifty is in a data set. The formula of IQRM is given by IQRM = Q_3-Q_1.

For example the length of AV when UE resides in the same tracking area from Time $\mathcal{T}_1$ to $\mathcal{T}_{11}$is shown in table 1.

Table 1: length of AV during UE resides in the same TA

Time	$\mathcal{T}_1$	$\mathcal{T}_2$	$\mathcal{T}_3$	$\mathcal{T}_4$	$\mathcal{T}_5$	$\mathcal{T}_6$	$\mathcal{T}_7$	$\mathcal{T}_8$	$\mathcal{T}_9$	$\mathcal{T}_{10}$	$\mathcal{T}_{11}$
Length AV	5	7	10	11	14	15	16	18	21	25	26

To find the IQRM for set of length of AVs which has been shown in above table. Assume at time $\mathcal{T}_{11}$only 17 records out of 26 are used and the UE is move to new tracking are. To predicate the length of AV in a new tracking. We need to put the number of records of AV which is consumed in ascending order (5, 7, 10, 11, 14, 15, 16, 17, 18, 21, 25) then find the median which is 15, then put the numbers below the median in group G1 = {5, 7, 10, 11, 14}, and the numbers above the median in group G2 = {16, 17, 18, 21, 25}. Compute the median for G1 which is 10 and median of G2 which is 18. This mean $Q_1 = 10$ *and* Q_3=18 , Then $IQR = Q_3\text{-}Q_1 = 18 - 10 = 8$. This mean the new length for AV in a new tracking area is 8. If the data set have even set of numbers then split the set into two groups G1 and G2 and find the median Q_1 for group 1 and the median $Q_3$for Group 2 and then $IQR = Q_3\text{-}Q_1$.

MODELING ANALYSIS BASED ON DYNAMIC LENGTH FOR AV

The authentication process is carried out in the following events: registration, incoming/outgoing call events. The registration event occurs when UE connects to the 4G mobile networks and when UE moves from on TA to new TA then TAU is carried out.

The UE sends N of Authentication Data Request to HSS through MME when the UE resides in the same TA. The HSS generates AV contains 5 records for each ADR. Then HSS send the authentication data response which includes AVs to MME. Each AV is suitable for one authentication and key establishment. The MME sends UAR for each user authentication request.

The events of registration (UE attach or TAU), incoming/outgoing call events are occurring at certain rate λ, randomly and independent. Therefore; the Poisson process is used to count these events. The Poisson process has the following probability mass function:

$$= \mathcal{P}(x,\lambda) = \frac{e^{-\lambda}\lambda^x}{x!} \; for \; x = 0,1,2,\ldots \qquad (1)$$

Where λ is the shape parameter which specifies the average number of events in the given time interval. The Poisson cumulative probability function is given by:

$$F(x,\lambda) = \sum_{i=1}^{x} \frac{e^{-\lambda}\lambda^i}{i!} \qquad (2)$$

Assume the following

1. UE resides from time $\mathcal{T}_{1,1}$to $\mathcal{T}_{\mathcal{N},1}$in the same tracking area TA,
2. UE generate n ADR
3. AV has $\mathcal{Q}$ records
4. UE leaves the TA at time $\mathcal{T}_{\mathcal{N},1}$.

The latest ADR is performed at time$T_{N,i}$, the MME uses only i records from last *AV*. The total number of UAR performed is given as:

$$x = (n-1) * \mathcal{Q} + i \; where \; (1 \le i \le \mathcal{Q}) \qquad (3)$$

The residence time for UE in the same TA is given as:

$$t = \mathcal{T}_{\mathcal{N},1} - \mathcal{T}_{1,1} \qquad (4)$$

The probability of there are n ADR in time $\tau$is given as:

$$\theta(n,\mathcal{Q},\tau) = \sum_{i=1}^{\mathcal{Q}} \left[\frac{(\lambda\tau)^x}{x!}\right] * e^{\lambda\tau} \qquad (5)$$

Assume the UE residence time t has general distribution form with mean$1/\mu$, the density function for UE residence time is represented by$f(t)$, and the Laplace transform is given as:

$$\ell\{f(t)\} = f^*(s) = \int_{t=0}^{\infty} f(t)e^{-st}dt \qquad (6)$$

The probability that there are n ADR when UE residences in the same TA is given as:

$$P(n,\mathcal{Q}) = \int_{t=0}^{\infty} \theta(n,\mathcal{Q},t)f(t)dt \qquad (7)$$

$$P(n,\mathcal{Q}) = \sum_{i=1}^{\mathcal{Q}} \int_{t=0}^{\infty} \left[\frac{(\lambda t)^x}{x!}\right] * \; e^{\lambda t} f(t)dt$$

$$= \sum_{i=1}^{\mathcal{Q}} \left[\frac{\lambda^x}{x!}\right] \int_{t=0}^{t=0} t^x * f(t)e^{-\lambda t}dt \qquad (8)$$

$$P(n,Q) = \sum_{i=1}^{\mathcal{Q}} \left[\frac{\lambda^x}{x!}\right] (-1)^x * \left[\frac{d^x f(s)}{ds^x}\right]\Big|_{S=\lambda} \qquad (9)$$

Assume $E[n]$ represents expected number of ADR when UE exist in in the same TA; then

$$E[n] = \sum_{n=1}^{\infty} n * P(n,Q) \qquad (10)$$

Let the residence time for UE in the same tracking area have gamma distribution. By using gamma distribution to represent the residence time for UE in the same TA. The gamma density function $\mathcal{F}(s)$ with mean $1/\mu$ and variance $\mathcal{v}$

$$\mathcal{F}(s) = (1+\mu v)^{-1/\mu^2 v} \qquad (11)$$

By using equation (11) we get:

$$\frac{d^x\mathcal{F}(s)}{ds^x} = (-\mu v)^n \left[\prod_{j=0}^{x-1}\left(\frac{1}{\mu^2 v}+j\right)\right](1 + \mu v s)^{-\left(\frac{1}{\mu^2 v}+x\right)} \quad (12)$$

By substituting equations (12 and 11) in 9 we obtain,

$$P(n,Q) = \sum_{i=1}^{Q}\left[\frac{(\lambda\mu v)^x}{x!}\right]\left\{\left[\prod_{j=0}^{x-1}\left(\frac{1}{\mu^2 v}+j\right)\right] * (1+\mu v\lambda)^{-\left(1/\mu^2 v+x\right)}\right\} \quad (13)$$

By using Equation (10) and substituting 13 in 10 to get $E[n]$ which represents expected number of ADR when UE resides in the same tracking area TA;

$$E[n] = \sum_{n=1}^{\infty} n * \sum_{i=1}^{Q}\left[\frac{(\lambda\mu v)^x}{x!}\right]\left\{\left[\prod_{i=0}^{x-1}\left(\frac{1}{\mu^2 v}+j\right)\right] * (1+\mu v\lambda)^{-\left(1/\mu^2 v+x\right)}\right\} \quad (14)$$

The cost of the total signaling transmission for ADR when UE resides in the same TA is given by:

$$C(Q) = E[N] * (Q * 2\alpha) \quad (15)$$

Where α represents the cost for $s6a$ signaling system messages between HSS and MME. By substituting equation 15 in 14 we get:

$$C[Q] = \sum_{n=1}^{\infty} n * \sum_{i=1}^{Q}\left[\frac{(\lambda\mu v)^x}{x!}\right]\left\{\left[\prod_{i=0}^{x-1}\left(\frac{1}{\mu^2 v}+j\right)\right] * (1+\mu v\lambda)^{-\left(1/\mu^2 v+x\right)}\right\} * (Q+2\alpha) \quad (16)$$

Let the UE residence time t in the same TA has exponential distribution and $\mu^2 v = 1$ then equation 13 can be simplified to:

$$P(n,Q) = \left(\frac{\lambda}{\lambda+\mu}\right)^{(n-1)*Q} * \left[1-\left(\frac{\lambda}{\lambda+\mu}\right)^{Q}\right] \quad (17)$$

$$E[n] = \frac{1}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^{Q}} \quad (18)$$

The total cost of transmission AV by using equation 15 is given by

$$C[Q] = \frac{Q+2\alpha}{1-\left(\frac{\lambda}{\lambda+\mu}\right)^{Q}} \quad (19)$$

PERFORMANCE ANALYSIS

A. GAMMA DISTRIBUTION RESIDENCE TIME

Figures 5 represents performance analysis when UE has gamma residence time distribution in MME with variance v. Assume UAR has arrival rate is λ = 15μ and the mean residence time is $1/\mu$. The results show the *E[N]* increases when variance *v* increases. This scenario is explained as follows: when the *v* increases, the MME residence is shorter, it is likely that $\mathcal{T}_{N+1} < \mathcal{T}_{1,2}$ in figure 3 and therefore *N=1* is expected. Also the figures 5 indicates that the *E[N]* is decreased when the authentication vector length *L* is increased. Therefore; the message signaling between mobile network entities and the network traffic are reduced.

Figure 6 show the relationships between the cost of total *ADRs* transmission *C(K)* and *E[N]*, The *C(K)* and *E[N]* are effected by arrival rate λ and the length L(AV).

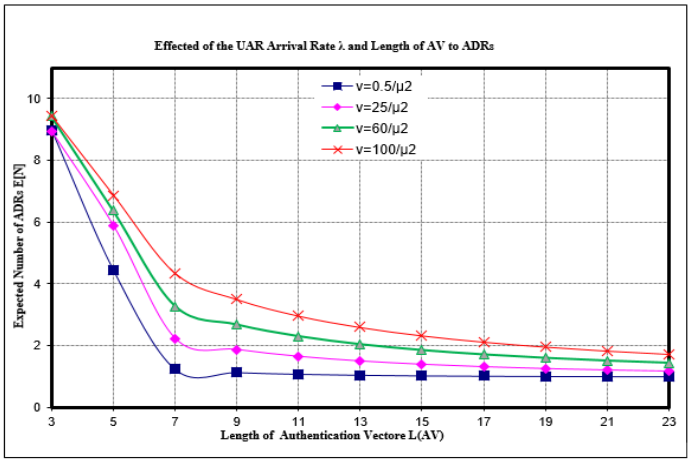

Figure 5: Effect of the UAR Arrival Rate λ (Gamma Residence λ=15μ)

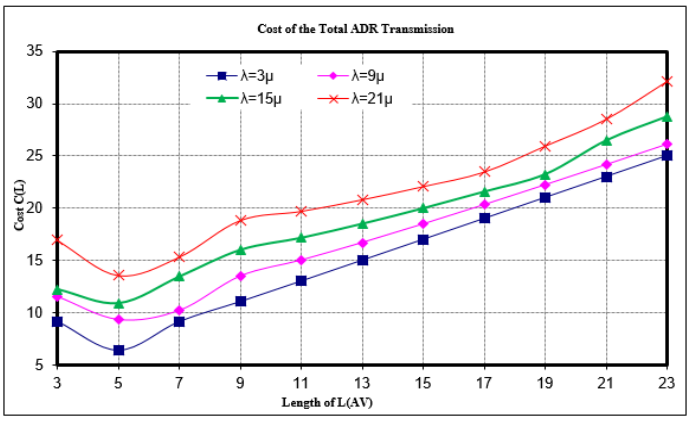

Figure 6: Cost of ADRs with Gamma Residence Times

When AV length increased then the ADRs will be decreased and the cost of transmission of AV will be increased. Figures 5 and 6 indicated there is optimal value for length of AV that depends on the arrival rate **λ** and residence times.

As shown in figure 5 when the length of authentication vector L is increased greater than the optimum value, The *E[N]* is not improved. This means that *E[N]* is fixed for large of authentication vector length.

B. EXPONENTIAL DISTRIBUTION RESIDENCE TIME

Figure 7 indicates the relationship UAR the length of AV and arrival rate. When MME has exponential distribution residence time with mean $1/\mu$. The results show that the E[N] is decreased when increasing the length of authentication vector. For large length AV the E[N] will be constant. This means insignificant to increase the L(AV) and the E[N] are a constant for large length of AV. Figure 8 shows that the cost of transmission AV will be increased with increasing the length of AV more than optimal value.

The proposed methods have average delay less than the existing method. Therefore; the suggested approaches have well performance and throughput than the current method, as presented in figures 9. In the current method the length of AV is fixed. This is not best choice, because this method is not predicate dynamic length for AV. The current technique does not depend on a study of the history of mobile movements and the arrival rate for events. But in the proposed method the history of mobile movements and the arrival rate for the event is considered in predict of the AV length. The average delay has enhanced significantly. The existing method has on average delay (5.2 ms); however, the AVM, IQRM which have been suggested by this research work are (3.9 ms) and (3.16 ms) respectively.

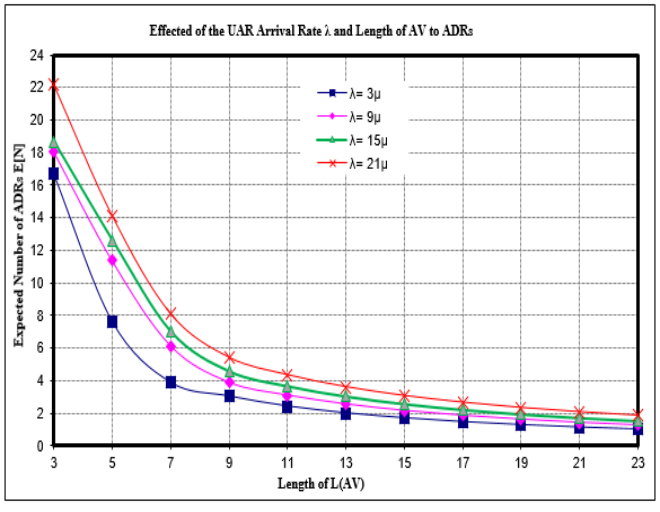

Figure 7: Effect of the UAR Arrival Rate λ (Exponential Residence)

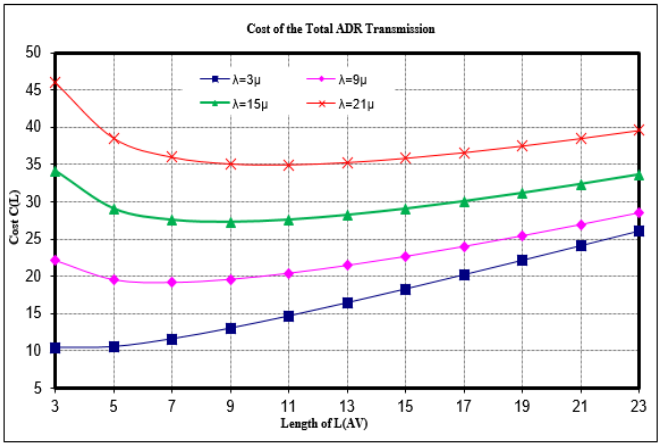

Figure 8: Cost of ADRs with Exponential Residence Times

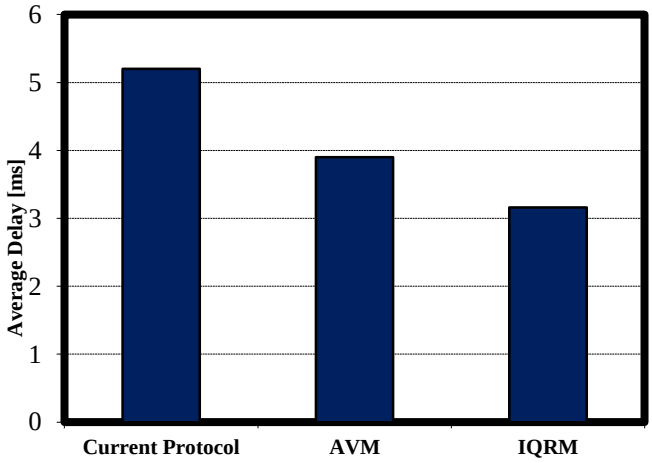

Figure 9: Average Delay

CONCLUSION

Authentication in the mobile network is performed in the following cases: registration- when UE connects to the 4G mobile networks and when UE moves from on Tracking Area (TA) to another one, and in incoming/outgoing call. In this cases, the cost of accessing the HSS is high, the MME must obtain a large number of authentication vectors at a time in order to reduce the number of accesses. However, if the size of the authentication vector increases, that is, if a large number of authentication vectors are transmitted at once, the cost of transmitting the authentication vector to MME becomes higher in each HSS. Also, when MME service area is terminated, the number of wasted authentication vectors also increases, which may result in a waste of signaling costs. Therefore, the appropriate value for length of authentication vector should be selected for the minimum authentication signaling cost. Through the proposed analysis model, we confirmed the following results:

- An increase in the value of L(AV) reduces the number of E[N]. However, when L(AV) is increased, the increased

L(AV) only shows a reduction of E[N] and does not reduce the cost of authentication signaling.

- A suitable L(AV) value for the UE's authentication event pattern indicates a decrease the authentication cost.

REFERENCES

[1] F.-Y. Leu, I. You, Y.-L. Huang, K. Yim, and C.-R. Dai, "Improving security level of LTE authentication and key agreement procedure," in *2012 IEEE Globecom Workshops*, 2012, pp. 1032–1036.

[2] R. K. S. and R. Singh, "4G LTE Cellular Technology: Network Architecture and Mobile Standards," *Int. J. Emerg. Res. Manag. Technol.*, vol. 5, no. 12, pp. 1–6, 2016.

[3] J. Al-Saraireh and S. Yousef, "Analytical model for authentication transmission overhead between entities in mobile networks," *Comput. Commun.*, vol. 30, no. 8, 2007.

[4] K. A. Alezabi, F. Hashim, S. J. Hashim, and B. M. Ali, "An efficient authentication and key agreement protocol for 4G (LTE) networks," in *2014 IEEE REGION 10 SYMPOSIUM*, 2014, pp. 502–507.

[5] S. Park, N. Kim, and Y. Jee, "An authentication mechanism for the UMTS-WiFi networks," in *Proceedings of the 6th International Conference on Mobile Technology, Application & Systems - Mobility '09*, 2009, pp. 1–4.

[6] A. Choudhary, "Analysis of UMTS 3G Authentication and Key Agreement Protocol AKA for LTE 4G Network," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 3, no. 4, pp. 2146–2149, 2015.

[7] Yi-Bing Lin and Yuan-Kai Chen, "Reducing authentication signaling traffic in third-generation mobile network," *IEEE Trans. Wirel. Commun.*, vol. 2, no. 3, pp. 493–501, May 2003.

[8] Yan Zhang and M. Fujise, "An improvement for authentication protocol in third-generation wireless networks," *IEEE Trans. Wirel. Commun.*, vol. 5, no. 9, pp. 2348–2352, Sep. 2006.

[9] L.-Y. Wu and Y.-B. Lin, "Authentication Vector Management for UMTS," *IEEE Trans. Wirel. Commun.*, vol. 6, no. 11, pp. 4101–4107, Nov. 2007.

[10] S.Arunkumar and P.Rajkumar, "Fast Re-Authentication for Efficient and Seamless Handover in 4G Networks," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 3, no. 4, pp. 1353–1358, 2014.

[11] M. Purkhiabani and A. Salahi, "Enhanced authentication and key agreement procedure of next generation evolved mobile networks," in *2011 IEEE 3rd International Conference on Communication Software and Networks*, 2011, pp. 557–563.

[12] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA," in *2009 Wireless Telecommunications Symposium*, 2009, pp. 1–8.

[13] V. Cristina-Elena, P. Victor-Valeriu, and B. Ion, "Security Analysis of LTE Access Network," *Tenth Int. Conf. Networks*, pp. 29–34, 2011.

[14] F. Hao and P. Ryan, "J-PAKE: Authenticated Key Exchange without PKI," Springer, Berlin, Heidelberg, 2010, pp. 192–206.

[15] X. Li and Y. Wang, "Security Enhanced Authentication and Key Agreement Protocol for LTE/SAE Network," in *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*, 2011, pp. 1–4.

[16] J. B. Bou Abdo, H. Chaouchi, and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for EPS," in *2012 Symposium on Broadband Networks and Fast Internet (RELABIRA)*, 2012, pp. 73–77.

[17] G. M. Koien, "Mutual entity authentication for LTE," in *2011 7th International Wireless Communications and Mobile Computing Conference*, 2011, pp. 689–694.

[18] Yu Zheng, Dake He, Weichi Yu, and Xiaohu Tang, "Trusted Computing-Based Security Architecture For 4G Mobile Networks," in *Sixth International Conference on Parallel and Distributed Computing Applications and Technologies (PDCAT'05)*, 2005, pp. 251–255.

[19] Yu Zheng, D. He, Xiaohu Tang, and Hongxia Wang, "AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform," in *2005 5th International Conference on Information Communications & Signal Processing*, pp. 976–980.

[20] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, "Providing Security in 4G Systems: Unveiling the Challenges," in *2010 Sixth Advanced International Conference on Telecommunications*, 2010, pp. 439–444.

[21] M. Prasada and R. Manoharanb, "Elgamal Signature based Authentication in LTE-Advanced," *Int. J. Inf. Process.*, vol. 7, no. 3, pp. 58–67, 2013.

[22] G. Wang, B.-S. Lee, and J. Y. Ahn, "Authentication and Key Management in an LTE-Based Unmanned Aerial System Control and Non-payload Communication Network," in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops*

(FiCloudW), 2016, pp. 355–360.

[23] C. Tang, D. A. Naumann, and S. Wetzel, "Analysis of Authentication and Key Establishment in Inter-generational Mobile Telephony," in *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing*, 2013, pp. 1605–1614.

[24] E.-A. Gin´es, C.-W. P. Raphael, and D. J. Parish, "Analysis and Design of Security for Next Generation 4G Cellular Networks," in *PGNeT 2012*, 2012, pp. 1–7.

[25] S. N., K. R., and M. Nithya, "Cryptography Key Initiator for 4G LTE Networks Using Session Keys," *Middle-East J. Sci. Res.*, vol. 24, no. 3, pp. 636–639, 2016.

[26] K. Shivali and S. Parvinder, "Security Enhancement of 4G LTE system using PGP and Iterative RSA technique," *Int. J. Eng. Comput. Sci.*, vol. 4, no. 9, pp. 14225–14229, 2015.

[27] K. Lee, J. Deng, and R. Sudhaakar, "Fast authentication in multi-hop infrastructure-based mobile communication," in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 665–670.

[28] R. Pradeepa, C. Lavanya, G. Rajalakshmi, and S. Kalaivani, "Security Enhancement In 4G Technology By Integrating SME and EPS Architecture," *Int. J. Adv. Res. Comput. Eng. Technol.*, vol. 4, no. 2, pp. 520–523, 2015.