International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518

Evaluation of Intrusion Prevention Technique in LTE Based Network

Eman F. El-Gaml, Hussein ElAttar, Hesham M. El-Badawy

Abstract— The motivation to reach fourth generation with high data rate throughout subscriber movement is the main goal of 3GPP Long Term Evolution/ System Architecture Evolution (LTE/SAE). The design of 3GPP LTE/SAE is to have purely IP-based architecture that creates a number of new challenges in designing the security mechanism against the risks, One of these challenges is to protect the subscriber authentication and communication from intruders when first attach to the LTE network and every time handover process occurs. However, because of the difficulty of warding off the IP-specific attacks and the complexity of cryptographic calculations we propose a mechanism oriented toward key revocation instead of reliance on a cryptographic function only. Handover key management in the 3GPP LTE/SAE has been designed to overcome the lack of privacy and insecure automatic key updates while minimizing signaling overhead on the network and computation delay by controlling the revocation process and determining the appropriate interval for operators to refresh the keys. Our main contribution, however, is to determine analytically the best description of the volume of exposed packets during the vulnerable period to help operators enhancing the prevention techniques on LTE networks without signaling overheads throughout different mobility schemes.

Index Terms— 3GPP authentication and key agreement (AKA), long term evolution (LTE), evolved packet system (EPS), mobile network security, handover key management.

1 Introduction

THE recent increase of mobile data usage and demand of new applications such as Multimedia Online Gaming, mobile TV, Web 2.0 and streaming contents, high data rates with quality of service through subscriber movement, have motivated the 3rd Generation Partnership Project (3GPP) to work on the Long-Term Evolution (LTE). LTE is the latest standard in the mobile network technology tree that previously realized the GSM/EDGE and UMTS/HSxPA network technologies that now account for over 85% of all mobile subscribers. LTE will ensure 3GPP's competitive edge over other cellular technologies [1] LTE, whose radio access is called Evolved UMTS Terrestrial Radio Access Network (E-UTRAN), is expected to substantially improve end-user throughputs, sector capacity and reduce user plane latency, bringing significantly improved user experience with full mobility. With the emergence of Internet Protocol (IP) as the protocol of choice for carrying all types of traffic, LTE is scheduled to provide support for IP-based traffic with end-to-end Quality of service (QoS). 3GPP is specifying a new Packet Core, the Evolved Packet Core (EPC) network architecture as shown in Fig. 1, to support the E-UTRAN through a reduction in the number of network elements, simpler functionality, improved redundancy but most importantly allowing for connections and hand-over to other fixed line and wireless access technologies, giving the service providers the ability to deliver high data rate with low latency. SAE/LTE, System Architecture Evolution (SAE) / Long-Term Evolution (LTE), went through several changes compared to 3G. These include the following: (a) the base station or enhanced NodeB (eNB) with enhanced functionality, (b) eNB is the end-point for the user traffic, (c) there is a key hierarchy allowing for key separation depending on the purpose, and (d) forward security is provisioned [2]. The Security implications of this flat architecture and allowing eNB placement in untrusted locations make it vulnerable to unauthorized access. The security designer's focus on preventing the expected risks on eNB's as much as they can, such as physical threats or by injection of software. The existing vulnerability could be in many aspects of the LTE security framework as follows: Vulnerability in LTE System Architecture, LTE Access Procedure, and LTE Handover Procedure. In this paper we focus on the threats that affect the hand over procedure and key management that the intruder could compromise session keys between eNBs during the handover of UE [3], [4] and how to recover from the security breaches faster to keep the attacker away from the core network. In the design consideration of Evolved Packet System (EPS), to make eNBs secure, there must be a separation between signaling and user data traffic. This new change implies not only physical separation paths for these two types of traffic but also separate key management for encryption and integrity protection. Setting up and configuring eNBs shall be authenticated and authorized [5] so that attackers shall not be able to modify the eNB settings and software configurations via local or remote access. Key management minimizes the security threats

- *Eman F. El-Gaml is currently pursuing masters degree program in electronics and Communications Engineering in the Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt. E-mail: eman.elgaml@gmail.com*
- *Hussein ElAttar is currently working as an assistant professor at the Arab Academy for Science, Technology and Maritime Transport, Cairo, Egypt . E-mail: attarh@hotmail.com*
- *Hesham M. El-Badawy, National Telecommunication institute (NTI), Cairo, Egypt. E-mail: heshamelbadawy@ieee.org*

International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518

through separation of session keys in handover between eNBs and keeps the compromised keys in one eNB. The most practical solution to reverse the effect of attack without overloading the network processes is to choose the optimal operational time for frequently refreshing the root key when detecting the compromised eNB. The acceptable tradeoff between signaling load and number of data packets exposed to attack during handing the keys off is the most important factor for service providers' network operators. We use the time diagram in [6] to measure the period during which a compromised key is operative and enhance the mathematical model to best fit the graph that helps operators to detect intrusions and then start the prevention techniques faster than older mechanism. The main contribution of this paper are fourfold: (1) In section 2, Review the effect of desynchronization attack on inter eNB handover, (2) Change the residence time assumption in the mathematical model process and explore the impact of other non-negative distribution processes such as log-normal distribution, and compare the results with gamma distribution results through key refresh process by considering system performance, as in section 3, then paper conclusion in section 4.

2 INTER ENB HANDOVER ATTACKS DETECTION AND PREVENTION

For efficient use of the air interface the eNB performs security-related key handling and algorithm negotiation during handover process, inter-eNB handover may involve the Mobility Management Entity (MME), or may not. In the design of not involving core network, keys would be passed in a manner that allow all eNBs in a "Hand Over, HO, chain" would know all the keys, this leads to one compromised eNB would compromise all eNBs in the "HO chain". By performing the backward key separation, i.e., One-way function used before key is passed, it blocks an eNodeB only from deriving past session keys from the current session key. For more secrecy, the forward key separation was introduce and MME involvement to produce fresh session keys to protect future session keys from being compromised. In this case, the Forward key separation will be effective after two hops. But when MME is already involved during the HO, Forward key separation is effective already after one hop. This process requires continuous synchronization between core network and eNBs, while the intruder could disrupt this synchronization and compromise all future keys between UE and subsequent eNBs, this is called desynchronization attacks which we are focusing on in this paper, by using a rogue eNB, an attacker can disrupt refreshing of the Next Hop Chaining Counter (NCC) value by either manipulating the handover request message between the eNBs or the S1 path switch acknowledgement message from an MME to a target eNB as described in Fig.1, messages 3 and 14 [5]. The KeNB is the key used between UE and source eNB, Next-Hop-KeNB is an intermediate parameter only used in KeNB* derivations. The KeNB* is the key used between UE and target eNB to derive

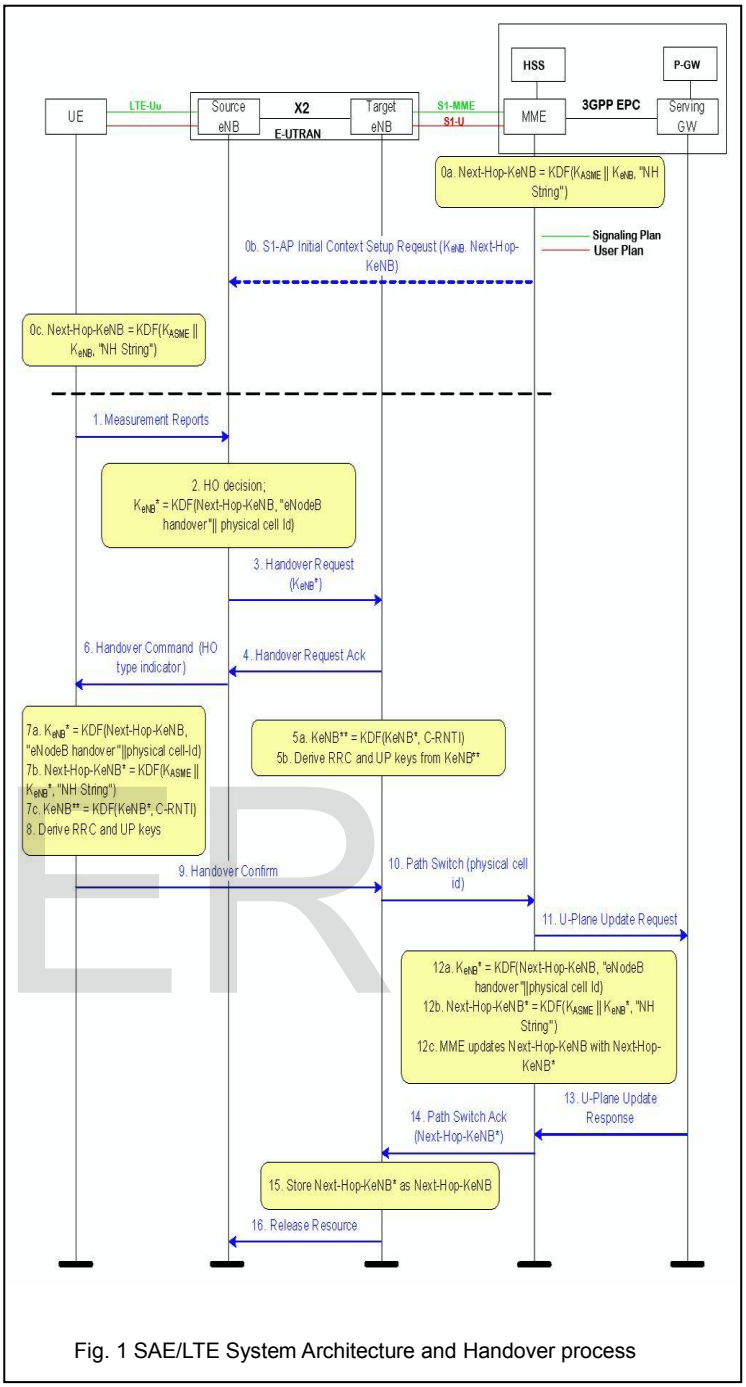


Fig. 1 SAE/LTE System Architecture and Handover process

KeNB** from target eNB C-RNTI (Cell Radio Network Temporary Identifier) and KeNB*. KeNB** is used to derive RRC (radio resources controller) and UP (user plan) keys. And C-RNTIIs identify the mobile within a cell. The target Cell Id is not be available for the UE in the HO Command message, but a physical cell Id is used instead. KASME (Key access security MME) is generated by HSS (Home Subscriber Server) and passed to MME. To desynchronize the NCC value in a targeted eNodeB, [6] the rogue eNodeB purposely sets an extremely high value for the NCC value and sends it to the targeted eNodeB in the handover request message in step (3) of Fig. 1. This extremely high value almost reaches the highest value permitted for an NCC value (i.e., 8 bits). An intruder

International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518

sends to a UE the original NCC value by synchronizing the false NCC value; ordering it not to perform key derivation. The NCC value from the S1 path switch acknowledgement (ACK) message is considerably smaller than that received from the rogue eNodeB, this size difference causes the targeted eNodeB and the UE to generate the next session key based on the current KeNB instead of the new Next Hop (NH) key. In such case, the compromised eNodeB possesses the further KeNB because the forward key separation of KeNB has been lost. The eNodeB acquiring this KeNB can now know the future KeNBs because this value can be exposed through the physical layer information [7]. After an initial desynchronization attempt, an adversary has to keep deceiving the UE into sending an original NCC value while continuing to track the UE for further active attacks. In this paper the prevention technique emphasizes the use of frequent root key update; because the attacker effect removed once the key refresh procedure is running with minimum cost on core network. Through detecting the time of attack, the operators can minimize the risk and manually refreshing the root key by using enhancing method as described in next section.

3 Analytical Modeling and Analysis

3.1 Analytical model for inter-eNodeB handover and keying updates

In this section we propose the analytical model of key update interval and how to manage the key refresh in different mobility schemes, the residence time is introduced with lognormal distribution rather than the gamma distribution used in [6]. First consider the timing diagram of an inter-eNB handover in term of a root key update. Fig. 2 illustrates a timing diagram [6] for one full MME residence time as determined by the time difference between entering and leaving an MME area($t_{RES} = t_l - t_e$) as shown in table 1 that indicate the parameter relations. Fig. 2 indicate the intra-MME handover (HO) and attack occurrence, the two notable incidents are as follows; the desynchronization attack at t_{desy} and expiration of root key update interval at $t_{exp/ref}$. When UE leave to new MME subnet at t_l or request manual key update at $t_{exp/ref}$, it minimizes the Desynchronization attack effect and mitigating the next update of the root key.

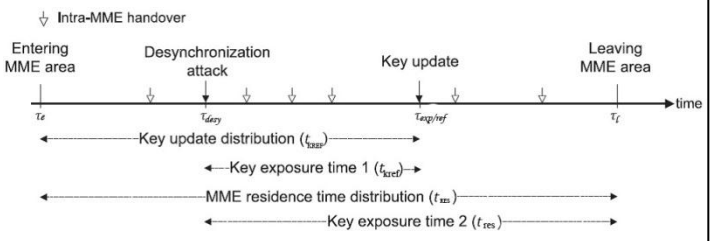


Fig. 2 Timing diagram of vulnerable period regarding MME residence time and key refresh interval [6]

Such a move or request triggers full EPS-AKA between an MME and a UE; as a result, the new K_{ASME} is agreed upon and a newK_{eNB} is derived from the freshK_{ASME}.

Once the desynchronization Attack is launched the current and future keys can be stolen by intruder until the next update of root key, the time difference between the attack occurrence and key refresh process is defined as vulnerable periodt_c. Whenever minimizing the period of detecting the attack the easier of mitigating, so t_c is calculated as the minimal time of the two exposure time, through finding the probability of the event occurring under range of time, by using cumulative distribution function we can describe the detection event occurring [6].

TABLE 1
PARAMETER DESCRIPTION AND RELATIONS

Parameter	Description and relations
t_{RES}	MME resident time ($t_{RES} = t_l - t_e$)
t_{res}	Key exposure time 1, the time from desynchronization attack at t_{desy} to leaving MME subnet ($t_l - t_{desy}$), residual time
t_{KREF}	Interarrival time of the key update "key refresh" ($t_{exp/ref} - t_e$)
t_{kref}	Key exposure time 2, the time from desynchronization attack at t_{desy} to key refresh period ($t_{exp/ref} - t_{desy}$), residual time
t_l	User leaving time
t_e	User entering time
t_{desy}	Desynchronization time
$t_{exp/ref}$	Key expiration time or key refreshing
t_c	Vulnerable period t_c=min{t_{kref}, t_{res}}, where 0≤ t_{kref}<t_{RES} and 0≤ t_{res}<t_{RES}
$f_{RES}(t), f_{res}(t), f_{KREF}(t), f_{kref}(t)$	Represent the probability density Functions (PDF) of t_{RES}, t_{res}, t_{KREF}, t_{kref}
$f^*_{RES}(s), f^*_{res}(s), f^*_{KREF}(s), f_{kref}(s)$	Represent the Laplace transforms of $f_{RES}(t), f_{res}(t), f_{KREF}(t), f_{kref}(t)$

The CDF of two independent random events, key update and MME residence can be expressed as follows:

$$\begin{aligned} F_c(t) &= Pr\{min(t_{res}, t_{kref}) \le t\} \\ &= Pr(t_{res} \le t) + Pr(t_{kref} \le t) \\ &\quad - Pr(t_{res} \le t).Pr(t_{kref} \le t) \end{aligned} \quad (1)$$

We can get the probability distribution function of t_c by differentiating both sides of (1) and then apply Laplace transform to both sides to simplify the process of analyzing the behavior of the system and solve the differential as in (2)

$$\begin{aligned} f^*_c(s) &= \int_0^\infty f_{res}(t).\left[\int_t^{t_{RES}} f_{kref}(\tau)d\tau\right].e^{-st}dt \\ &\quad + \int_0^\infty f_{kref}(t).\left[\int_t^{t_{RES}} f_{res}(\tau)d\tau\right].e^{-st}dt \\ &= f^*_{res}(s) + f^*_{kref}(s) \\ &\quad - \int_0^\infty e^{-st}.f_{res}(t).\int_0^t f_{kref}(\tau)\,d\tau\,.dt \\ &\quad - \int_0^\infty e^{-st} f_{kref}(t).\int_0^t f_{res}(\tau)\,d\tau \end{aligned} \quad (2)$$

According to the paradox of residual life [8], the residual time or exposure time distribution of an original distribution is not equivalent to the original distribution. The residual time, γt, is defined as the time from t to the next arrival if t is an arbitrary

International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518

point in the original renewal process, R_t. The PDF of residual time in the Laplace form, $f_\gamma^*(s)$ is calculated by the residual life theorem [8] as shown in (3), where $f_{RES}^*(s)$, and $E(R_t)$ represent the Laplace transform of PDF and the expectation value of the original renewal process R_t.

$$f_\gamma^*(s) = \frac{1 - f_{RES}^*(s)}{S.E(R_t)} \quad (3)$$

A Poisson process is known as a counting process for which the inter-arrival times between events are independent and identically distributed (i.i.d), exponential random variables [9]. One possible generalization is to consider a counting process for which the times between successive events are i.i.d with an arbitrary distribution. Such a counting process is called a renewal process. The PDF of the key update interval and the Laplace transform are in (4), where $\mu_u = 1/ T_U$, and T_U is the mean value. According to (3), the Laplace transform of $f_{kref}(t)$ is calculated as follows:

$$f_{kref}^*(s) = \frac{1 - f_{KREF}^*(s)}{s.\int_0^\infty t\,.f_{KREF}(t).dt} = \frac{\mu_u}{S+\mu_u} \quad (4)$$

Through its Laplace transform, we can deduce that the PDF of the exposure time of the key update, $f_{kref}(t)$, would follow the exponential distribution. We expand $f_c^*(s)$ in (2) as shown in (5)

$$f_c^*(s) = \frac{\mu_u}{S+\mu_u} + \frac{S}{S+\mu_u}\,.f_{res}^*(s+\mu_u) \quad (5)$$

Recently available data obtained from [6] assumes the distribution of the MME residence time follows a gamma distribution accordingly, we will now try to find an expression for the expected volume of exposed packets during vulnerable period using lognormal distribution to describe the MME residence time in a more facilitated and general cases. The PDF and Laplace of the MME residence time is shown in (6)

$$\mathcal{L}\{f_{RES}(t,\mu,\sigma)\} = \mathcal{L}\left\{\frac{1}{t\sigma\sqrt{2\pi}}\bar{e}^{\frac{(logt-\mu)^2}{2\sigma^2}}\right\} \quad (6)$$

Since closed form expression of Laplace transform for lognormal distribution don't exist, the author in [10] analyze a closed-form approximation $\tilde{\mathcal{L}}(\theta)$of the Laplace transform of $\mathcal{L}(\theta)$

$$\tilde{\mathcal{L}}(\theta) = \frac{\bar{e}^{\frac{(W^2(\theta\, e^\mu\, \sigma^2)+ 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}}{\sqrt{I + W(\theta e^\mu\, \sigma^2)}}\,, \theta \in R^+ \quad (7)$$

Where w is the lambert function [10] which is defined as the solution of the equation $w(t)e^{w(t)} = t$, "o" is asymptotic order, and $\tilde{\mathcal{L}}(\theta)$ is Laplace approximation of moment generating functions, and is defend as follow:

$$\tilde{\mathcal{L}}\,\{\theta\} = \tilde{\mathcal{L}}\,(\theta)(1 + olog^{-1}(\theta))$$

Therefor the Laplace transform of the resident time PDF is:

$$f_{RES}^*(s) = \frac{\bar{e}^{\frac{(W^2(\theta\, e^\mu\, \sigma^2)+ 2w\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}}{\sqrt{I + W(\theta e^\mu\, \sigma^2)}} \quad (8)$$

Where μ and σ are the shape and scalar parameters of lognormal distribution, Then from (3)

$$f_{res(s)}^* = \frac{1 - f_{RES}^*(s)}{sE(R)} = \frac{1 - f_{RES}^*(s)}{se^{\mu+\sigma^2/2}}$$

$$= \frac{1 - \frac{\bar{e}^{\frac{(W^2(\theta\, e^\mu\, \sigma^2)+ 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}}{\sqrt{I+W(\theta e^\mu\, \sigma^2)}}}{se^{\mu+\sigma^2/2}}$$

$$= \frac{\sqrt{I + W(\theta e^\mu\, \sigma^2)} - \bar{e}\,\frac{(W^2(\theta\, e^\mu\, \sigma^2) + 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}{se^{\mu+\sigma^2/2}\sqrt{I + W(\theta e^\mu\, \sigma^2)}} \quad (9)$$

From (9) we compute (5) as follows:

$$f_c^*(s) = \frac{\mu_u}{s+\mu_u} + \frac{s}{s+\mu_u}\left[\frac{\sqrt{I + W(\theta e^\mu\, \sigma^2)} - \bar{e}\,\frac{(W^2(\theta\, e^\mu\, \sigma^2) + 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}{(s+\mu_u)e^{\mu+\sigma^2/2}\sqrt{I + W(\theta e^\mu\, \sigma^2)}}\right]$$

$$= \frac{\mu_u}{s+\mu_u} + \frac{s}{(s+\mu_u)^2}\left[\frac{\sqrt{I + W(\theta e^\mu\, \sigma^2)} - \bar{e}\,\frac{(W^2(\theta\, e^\mu\, \sigma^2) + 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}{e^{\mu+\sigma^2/2}\sqrt{I + W(\theta e^\mu\, \sigma^2)}}\right] \quad (10)$$

The expected volume of exposed packets during the vulnerable period, E(N) is defined as follows:

$$E(N) = \lambda_p\,[-\frac{d}{ds}f_c^*(s)|s = 0]$$

$$=\lambda_p\left[-\frac{1}{\mu_u} + \frac{1}{\mu_u^2}\left[\frac{\sqrt{I+W(\theta e^\mu\, \sigma^2)}-\bar{e}\,\frac{(W^2(\theta\, e^\mu\, \sigma^2)+ 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}{e^{\mu+\sigma^2}\sqrt{I+W(\theta e^\mu\, \sigma^2)}}\right]\right] \quad (11)$$

The distribution of interarrival time between key [6] renewals, $f_l(t)$, is the convolution of $f_{KREF}(t)$ and $f_{RES}(t)$. The Laplace transform of $f_l^*(t)$ can be calculated as in (12) and the expected value of the signaling overhead rate, E(S) is calculated in (13)

$$f_l^*(s) = f_{KREF}^*(s).f_{RES}^*(s) = \frac{\mu_u}{s+\mu_u}.f_{RES}^*(s)$$

$$= \mu_u\bar{e}\,\frac{\frac{(W^2(\theta\, e^\mu\, \sigma^2) + 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}{(s+\mu_u)\sqrt{I + W(\theta e^\mu\, \sigma^2)}} \quad (12)$$

$$E(S) = \rho/-\frac{d}{ds}(f_l^*(s))|s = 0$$

$$= \rho/\left[\mu_u\,\frac{\bar{e}^{\frac{(W^2(\theta\, e^\mu\, \sigma^2)+ 2W\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}}{(s+\mu_u)^2\sqrt{I+W(\theta e^\mu\, \sigma^2)}}\right]|_{s=0} \quad (13)$$

$$E(S) = \frac{\rho\mu_u\sqrt{I + W(\theta e^\mu\, \sigma^2)}}{\bar{e}\,\frac{(W^2(\theta\, e^\mu\, \sigma^2) + 2w\,(\theta\, e^\mu\, \sigma^2)}{2\sigma^2}}$$

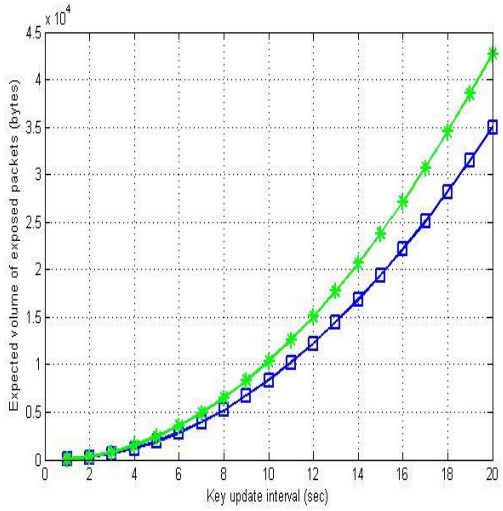
Where λ_p in (10) is the mean arrival rate of packets and equal to 64 Kbps, and ρ in (13) denotes the number of bits in

International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518

messages for individual authentication among the UE, the MME, and the HSS/AuC and it is equal to 384 bytes

3.2 Analysis of Expected exposure packet and signaling overheads with lognormal distribution during vulnerable period

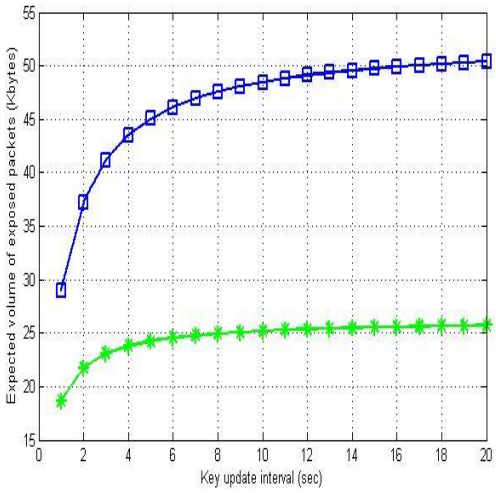
Generally as shown in Fig. 3, and Fig. 5, as the mean value of gamma distribution T_U increases, E(N) increases, and E(S) decreases, while when the mobility rate μ_r increases the E(N) decreases and E(S) increases, because high mobility implies frequent changes of the MME areas and, hence, frequent performing of the EPS-AKA of the inter-MME handover and vice versa. As shown in Fig. 4 and Fig. 6, the σ parameter in case of lognormal distribution represent the required time for any displacement, in other word 1/σ is deployed in current model to investigate the mobility effect in the key refresh process. Since μ_r and σ are inversely proportional to each other [11], the obtained system behavior will be matched to that presenting in [6]. However it can be noted that in the Gamma distribution in Fig. 3, the expected volume of exposed packet increase as the key update interval increase and then it saturates. We note that the corresponding in Fig. 4, indicates that using lognormal distribution shows that as the key update interval increases the expected volume of exposed packet will still increasing accordingly. It implies that the lognormal distribution is better in fitting longer update intervals without overhead on networks due to its heavy-tail characteristics. Selection of an appropriate root key update interval should be a high priority for network administrators that brings E(N) and E(S) to their lowest possible values that mean balance between signaling overhead and risk of security breaches.



□ σ =1, * σ =2

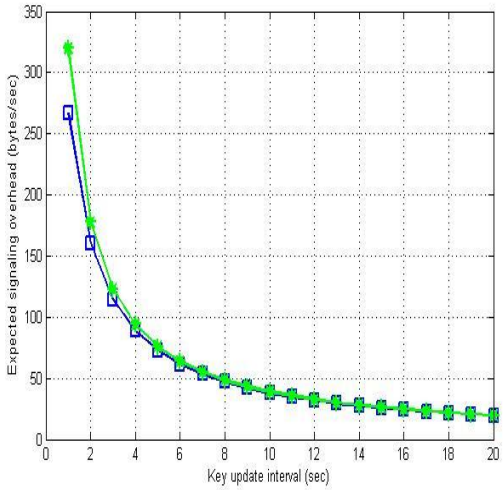
Fig. 4 Expected volume of exposed packet over the key update interval T_U using Log-normal distribution

It is not only the mobility rate that can affect the analytical model of MME residence distribution but also is affected by other factors, like Inter-eNodeB distance (deNB) or the size of MME area under the same constraints of user movement and Road characteristics (cROAD). That model helps operators to prevent the intruder as much as they can.



□ μ_r=1, * μ_r=2

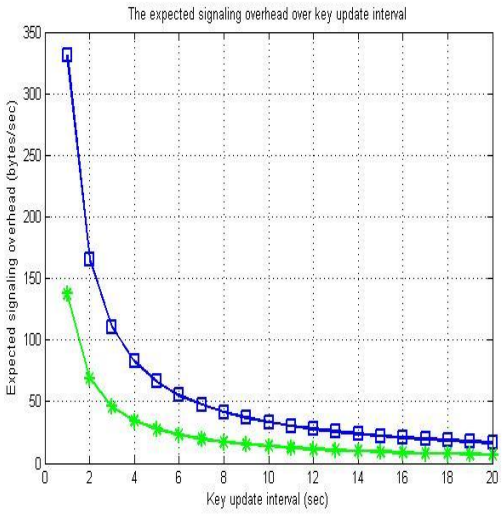
Fig. 3 Expected volume of exposed packet over the key update interval T_U using Gamma distribution



□ μ_r=1, * μ_r=2

Fig. 5 Signaling overhead in case of Gamma distribution

International Journal of Scientific & Engineering Research, Volume 5, Issue 12, December-2014
ISSN 2229-5518



□ σ =1, * σ =2

Fig. 6 Signaling overhead in case of Log-normal distribution

Using the lognormal distributions model is more suitable for fitting the residence time distribution than in the Gamma model and it provides a good approximation to be beneficial when modeling packet loss with key update interval.

4 Conclusion

In this paper, we deliver a review of LTE handover key management security procedure and we were concerned with the threats on forward key separation in handover key management, and how to describe the packets exposed to desynchronization attack using different distribution functions to select an optimal handover key update interval that helps network operators to enhance the detection and prevention techniques.

Using the lognormal distributions model is more suitable for fitting the residence time distribution than in the gamma model and it provides a good approximation to be beneficial when modeling packet loss with key update interval.

References

[1] Motorola, "Long-Term Evolution (LTE): Long Term Evolution (LTE): A Technical Overview," technical white paper, 2007.

[2] Anand R. Prasad and Xiaowei Zhang, " Overview of SAE/LTE security," IEEK Transactions on Smart Processing and Computing, vol. 2, no. 1, Feb 2013.

[3] D. Forsberg, "LTE Key Management Analysis with Session Keys Context," ELSEVIER Computer Comm., vol. 33, no. 16, pp. 1907 1915, Oct. 2010.

[4] G. Horn, "LTE Security", first ed. Wiley-Interscience, Nov, 2010.

[5] "3GPP System Architecture Evolution (SAE); Security Architecture (Release 8)," 3GPP TS 33.401, Version 8.0.0, June 2008.

[6] Chan-Kyu Han, Hyoung-Kee Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks," IEEE transactions on mobile computing, vol. 13, no. 2, Feb 2014

[7] D. Forsberg et al., "Enhancing Security and Privacy in 3GPP EUTRAN Radio Interface," Proc. IEEE 18th Int'l Symp. Personal, Indoor and Mobile Radio Comm. (PIMRC), Sept. 2007.

[8] L. Kleinrock, Queueing Systems: Theory, vol. 1, first ed. Wiley- Interscience, Jan. 1975.

[9] Chan-Kyu Han, Hyoung-Kee Choi, Jung Woo Baek, Ho Woo Lee, "Evaluation of Authentication Signaling Loads in 3GPP LTE/SAE Networks" , "IEEE Trans. Local Computer Network, Oct 2009, doi: 10.1109/LCN.2009.5355157"

[10] Soren Asmussen, Jens Ledet Jensen, Leonardo Rojas-Nandayapa, "On the Laplace transform of the Lognormal distribution", November 19, 2013.

[11] Debasis Kundu¤& Anubhav Manglicky, "Discriminating Between The Log-normal and Gamma Distributions",Department of Mathematics, Indian Institute of Technology Kanpur, Pin 208016, INDIA.