www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 9 Sep 2015, Page No. 14225-14229

Security Enhancement of 4G LTE system using PGP and Iterative RSA technique

Shivali Kanwal, Parvinder Singh

Department of Electronics and Communication,
RIET, Ropar
kanwal.shivali26@gmail.com
Department of Electronics and Communication,
RIET, Ropar
er.parvinder@gmail.com

Abstract: ***Security is often vital in knowledge networks; however it's significantly crucial in wireless networks like LTE. One in all the distinctive challenges of fourth-generation technology is the way to shut a security gap through that one compromised or malicious device will jeopardize a whole mobile network due to the open nature of these networks. To satisfy this challenge, relinquishing key management within the 3GPP LTE/SAE has been designed to nullify any vulnerable keys and as a result detach tainted network devices. Though periodic updates of the PGP key are Associate in Nursing integral a part of relinquishing key management, our work here emphasizes however essential these updates or to minimizing the result of asynchrony attacks that, as of now, can't be effectively prevented. The main contribution, however, is to explore however network operators will verify for themselves Associate in Nursing best interval for updates that minimizes the communication load they impose ,whereas protective for the protection of user mobility. Our rational and simulation consideration indicate the impact of the key update interval on such performance criteria as constellation and user quality once victimization RSA and PGP.***

Keywords: 4G LTE/SAE, Session key, RSA, PGP.

1. Introduction

LTE, Associate in nursing initialize of long evolution, marketed as 4G LTE, may be a normal for wireless communication of high-speed knowledge for mobile phones and knowledge terminals. It's supported the GSM/EDGE and UMTS/HSPA network technologies. It's aiming for max a hundred Mbps downlink and fifty Mbps transmission speed once victimization twenty megacycles per second information measure in order that it will modify various mobile multimedia system service provisions. The quality is developed by the 3GPP that is third Generation Partnership Project.

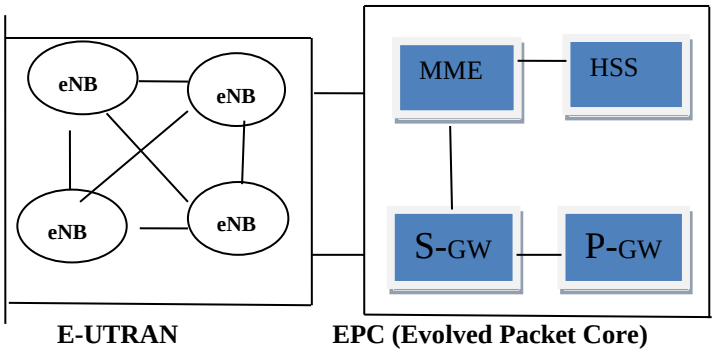


Figure 1: LTE –System Architecture Evolution (SAE)

Figure 1 below shows the LTE high level architecture [21]. The UE (user equipment) like mobile phones or Laptops attach or connects to the wireless through the E-UTRAN (Evolved UMTS Terrestrial Radio Access Network). After that E-UTRAN get connect to the EPC (Evolved Packet Core) which is IP-based and then connects to the provider wireless IP network. Unlike 3G wireless system, the LTE network architecture has a number of key differences.

Firstly, it consists of less network elements (NEs) i.e.:1) eNodeB, enhanced base station and 2) the required for the EPC. Secondly, LTE supports messed Access Gateway (AGW), have all the functions architecture with greater efficiency and performance gains. The eNB is single type of system in 4G E-UTRAN which have all the radio interface-functions for LTE. Also AGW is single type system in LTE EPC. consist multiple modules like HSS (home subscriber server), P-GW (Packet Data Network Gateway), S-WG (Serving Gateway), MME (Mobility Management Entity). LTE standard is flexible to allow vendors to combine all these modules to single or multiple device. MME is key control- node for the LTE which manages the UE identity along with mobility and security authentication. It selects SGW for UE during initial network formation and LTE handover, also authenticate user by communicating with HSS. Thus MME handles security key management function in LTE system.The S-WG bounces the interface to the E-UTRA. S-WG has key responsibility to send and lead data packets. The P-WG leads interface to packet data network.

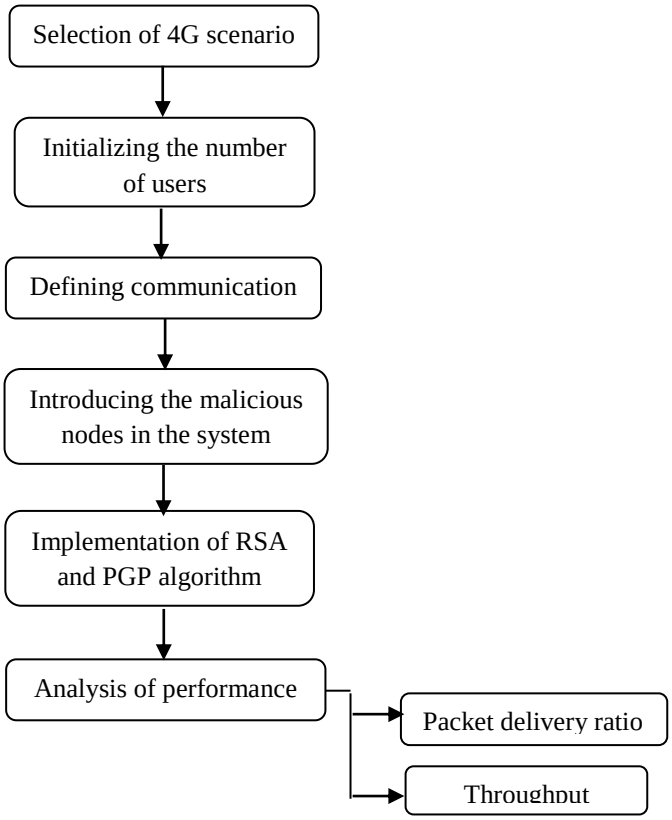
It is the gateway responsible for communication between UE and devices far from SP main IP network. The HSS maintains information per-user and responsible for subscriber management and security. It also contains information for subscription that allows network entities to handle call sessions. HSS generates acknowledge data and pass it to MME. After that there is a challenge-response and key arrangement steps between the MME and the UE .At the end HSS combines with the EPC based on the IP-based diameter protocol not with SS7 protocol used in earlier communication networks.

In this paper there is a tendency to tend to gift associate in nursing overall vision of the 4G networks starting by presenting variety of the key choices they will supply, thus discussing key challenges the researchers and vendors try and resolve, and eventually in short describing variety of the planned solutions to those problems.

2. BACKGROUND

Within the cable TV business, the expansion to 4G Networks may well be a really real likelihood in 2009. Recently, Comcast and T-Mobile have collaborated and in agreement to the event of a mobile 4G network to be tested in Washington D.C. and concrete center, MD [11]. However, this technique is extended, and thus the rollout of such a network is not expected for close to two years, as a result of the network wants thorough and elaborate testing thus on ensure that there are not any bugs that will interrupt the flow of mobile traffic across the network [11]. This type of likelihood is of essential importance in developing a network that is capable of advancing technology to never-before-seen heights. Similarly, AT&T, one altogether the world's largest telecommunications suppliers, will begin its own rollout of a 4G Network in 2011, sanctionative its Brobdingnagian user base to explore new downloading speeds and capabilities [18]. The use of LTE mobile broadband technology may be likelihood for the corporation to expand its horizons into 4G territory, upstaging current 3G capabilities [18]. Among the tactic of accelerating into the new 4G enterprise, AT&T will seek for to beat any limitations brought on by the 3G Network technique. As AT&T begins its rollout technique, there are a unit many considerations involved in guaranteeing that the transition may well be successful, that existing networks do not appear to be interrupted among the technique to establish the 4G platform. Further, mobile suppliers like AT&T will attainable develop new analysis ways in which from variety of their most popular product, alongside the iPhone, in response to the challenges of developing faster networks [21].The 4G Network technique wants a singular approach to developing effective models for strategic functions. the necessity for 4G networks is expounded to the improved utilization of data websites such as you Tube and Facebook, that require tremendous system of measurement thus on be used successfully [10]. As a results of these websites became. Increasingly well-liked amongst the ultimate public, it is a heap ofnecessary than ever for telecommunications suppliers to develop opportunities to accommodate the necessities of the customer population. Shoppers have return to rely upon utterly totally different supply's of data as a supply of recreation and for convenience. Therefore, it is necessary that organizations like Verizon and AT&T still establish sq. measures where technological enhancements are required.In Gregorian calendar month 2009, the first operative 4G Network was established by a venture between Clear wire and Intel, that reflected an opportunity for residents and businesses in Portland, state connect wirelessly anywhere in Portland at high broadband data rate. However, with the technology quickly approaching a widespread rollout, many cities, states, and countries will presently possess similar capabilities, as shoppers and businesses alike are given utterly totally different opportunities to expand their networks and interfaces with advanced capabilities. Moreover, it's evident that the Clear wire strategy is not whereas not its disadvantages and additional efforts ought to be created to beat any technology-related problems which can persist before a widespread rollout is even thought of.

3. Simulation



Flow chart 1: Proposed Method

DOI: 10.18535/ijecs/v4i9.27

In this analysis work is finished on the safety of 4G/SAE. According Flow chart, Foremost state of affairs is formed then nodes area unit initialized then for the implementation RSA and PGP is employed that stands for intrusion detection system and that we area unit exploitation hybrid model. It typically accustomed alert the system concerning the approaching danger.

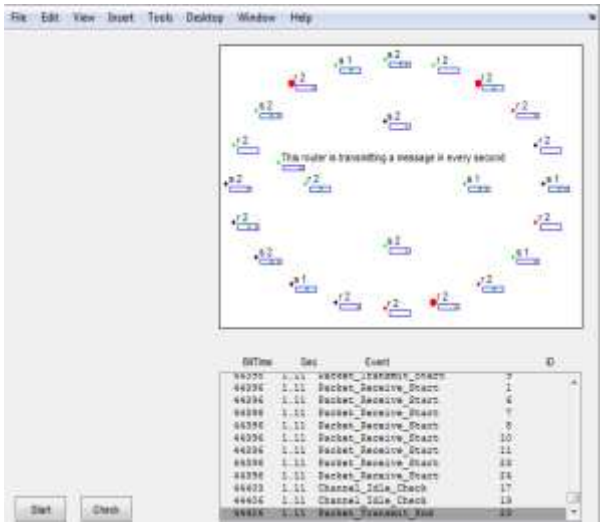


Figure 2 : 4G/SAE Scenario

Here, projected methodology is alerting different nodes concerning the malicious node. At the tip the comparison is finished between previous ways.

3.1 Proposed Hybrid Algorithm

When a user encrypts data (Ack) with PGP, PGP first compresses the data (Ack). Data compression, among the things, strengthens cryptographic security because it diminishes the arrangement found in languages. PGP then creates a session key; this key is a random number generated from the movements of the user's mouse and the key strokes being typed. Then the random number is run through a symmetric encryption algorithm with RSA, which generates a one-time-only secret key. The session key works with a very reliable and symmetric encryption algorithm to encrypt the data (Ack); the result is cipher text. Once the data is encoded, the session key is then encrypted to the recipient's public key, using asymmetric encryption RSA. Encryption and Decryption using RSA. The RSA scheme is a block cipher in which the data (Ack) and cipher text are integers between 0 to n-1 for some n. The steps for encryption and decryption are as follows [1]

Step 1: select two prime's p and q.

Step 2: calculate n= p*q

Step 3: calculate Ø (n) = (p-1) (q-1)

Step 4: select e such that e is relatively prime to Ø (n).

Step 5: calculate d such that d= mod (Ø (n))

Step 6: calculate c; C = M mod n

Step 7: calculate M = Cd mod n.

Thus the obtained key is encrypted by using the RSA algorithm to send through the channel and finally it is digitally signed by using session key algorithm.

Figure 3 : Intrusion Node Detected

A session key is an authentication mechanism that enables the creator of a key to attach a code that acts as a key. The key is formed by taking the hash of the key and encrypting the key. The key guarantees the source and integrity of the key. The signing of a key is done by the private key of the user [1]. For this purpose Elliptic Curve Session key algorithm is adopted for signing a message m by sender S using A's private key, SA. This message detects malicious node shown in Fig 3. So the concatenated and encrypted messages along with the values of r and s key pair keys are sent through the channel. The receiver must decrypt and separate the message and does the verification process. The steps are as follows.

Step 1: e= h (m)

Step 2: select a random integer k from [1 n-1]

Step 3: calculate r =x1(mod n)

Step 4: s = (1/k)(e + SA x r)(mod n).

The key pair is (r, s). The steps of verification for user B to authenticate user A are as follows,

Step 1: Verify whether r, s are in [1, n-1]

Step 2: Calculate e= hash (m)

Step 3: Calculate w=(1/s)(mod n)

Step 4: u1 = e x w (mod n) & u2 = r x w (mod n)

Step 5: Calculate (x1, y1) = u1x G + u2 x QA

Step 6: The key is valid if x1 = r (mod n).

Thus the key is authenticated and verified and malicious node information can be broadcast Fig4.

DOI: 10.18535/ijecs/v4i9.27

Figure 4 : Update intrusion Information

3.2 Key Update Method

Selection of associate degree acceptable PGP key update interval ought to be a high priority for network directors. Associate degree unnecessarily frequent key update interval wastes signal overhead. On the opposite hand, an unenergetically rare key update interval could finish anger associate degree end user's security and solitude. To search out associate degree optimum operational purpose for a PGP key update interval that may minimize each the quantity of exposed packets and therefore the signal traffic overhead. In step with [8], the optimum worth could lie on the balanced worth between 2 decisive factors once they have inverse relationship. It tends to outline associate degree optimum worth in concert with that, with a given vary of TU, network operators will operate their systems with a balance between signal overhead and risk of security breaches; in different words, such a price incorporates a most TU that brings E½Nand E½Sto their lowest potential values. However, in general, a globally accepted balanced worth doesn't exist as a result of such a price ought to be determined by a network operator and should take management PGP into consideration. Thus, we wish to produce network operators with associate degree choice to offer completely different load, likewise with the management plans, to E½Nand E½Sin the course of determinative a correct TU worth.

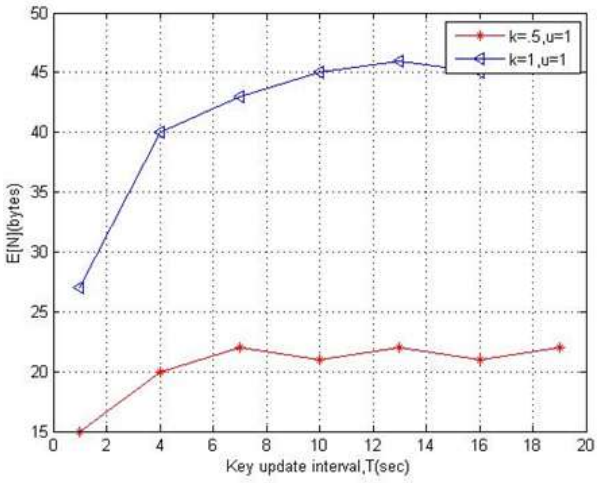


Figure 5 : Key update interval vs transmitted Data

4. Result

The result of a Key Update Interval on the Vulnerable Period figures.

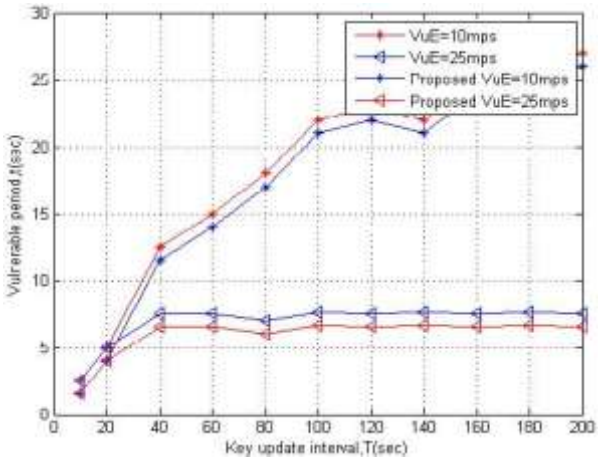


Fig 6 : key update vs vulnerable time (wrt speed)

In Figure 6 depicts the vulnerable amount (tc) versus the key update interval in terms of security, severally Note that the vulnerable amount corresponds to the minimum of 2 parameters: MME duration and therefore the key update interval. If the MME duration is fastened, because the key update interval worth will increase, vulnerability is greatest at the purpose once the key update interval worth equals the MME duration. Thus, any worth for the key update that's bigger than the purpose at that this most vulnerability happens is unnecessarily long, even once a less frequent key update would serve to cut back signal overhead.

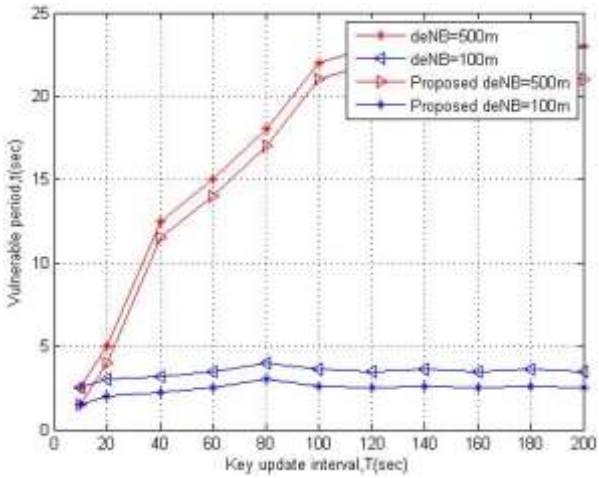


Figure 7: key update vs vulnerable time (wrt distance)

In Figure7, confine our attention to a set deNB (100 m). We tend to didn't concentrate on the link among performance criteria. However, in reality, a hybrid algorithm {in during a associate degree exceedingly a very} geographical area would possibly move quicker than one in an populated area owing to less congestion and better speed limits. Besides, the inter-eNodeB distance and populated area is also shorter

than in a geographical area owing to synthetic obstacles in a populated area that will interfere with signal propagation. However, we tend to check however our assessment balanced with physical world operations by manually analyzing the inter-eNodeB distance of Verizon. Once visually inspecting the inter-eNodeB distance, we tend to terminated that the relationship of freelance performance factors is simply too unsure for precise definition. As a result, we tend to place the responsibility on a network operator to gain associate degree optimum interval for change a hybrid key. This determination ought to be supported the operator's examination of a personal security.

5. CONCLUSION

This paper, involved the hybrid key separation in relinquishment key management within the 3GPP LTE/SAE network will be vulnerable owing to what area unit called scalawag base station attacks. Though sporadically change the hybrid key minimizes the result of the attacks, choosing associate degree optimum key update interval is associate degree unclear drawback owing to the problem of achieving a balance between the signal load and therefore the volume of exposed packets. we've got hybrid algorithm associate degree optimum relinquishment key update time that aid a network operator chose associate degree optimum worth that matches best with network management policies.

REFERENCES

[1] "3GPP System Architecture Evolution (SAE); Security Architec- ture (Release 11)," 3GPP TS 33.401, Version 11.2.0, Dec. 2011.

[2] "3G Security, Security Architecture (Release 8)," 3GPP TS 33.102, Version 11.1.0, Dec. 2011.

[3] M. Zhang et al., "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol," IEEE Trans. Wireless Comm., vol. 4, no. 2, pp. 734-742, Mar. 2005.

[4] C.B. Sankaran, "Network Access Security in Next-Generation 3GPP Systems: A Tutorial," IEEE Comm. Magazine, vol. 47, no. 2, pp. 84-91, Feb. 2009
.
[5] V. Niemi et al., "3GPP Security Hot Topics: LTE/SAE and Home (e)NB," Proc. ETSI Security Workshop, Jan. 2009.

[6] Y. Park et al., "A Survey of Security Threats on 4G Networks," Proc. IEEE GlobeCom Workshop Security and Privacy in 4G Networks, Nov. 2007.

[7] I. Bilogrevic et al., "Security and Privacy in Next Generation Mobile Networks: LTE and Femtocells," Proc. Int'l Femtocell Workshop, June 2010.

[8] Y.-B. Lin et al., "One-Pass GPRS and IMS Authentication Procedure for UMTS," IEEE J. Selected Areas in Comm., vol. 23, no. 6, pp. 1233-1239, June 2005.

[9] Y.-B. Lin et al., "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network," IEEE Trans. Wireless Comm., vol. 2, no. 3, pp. 493-501, May 2003.

[10] H. Yangzhi et al., "An Improved Authentication Protocol with Less Delay for UMTS Mobile Networks," Proc. IEEE Int'l Conf. Networking and Digital Soc. (ICNDS), May 2009.

[11] J.-A. Saraireh et al., "A New Authentication Protocol for UMTS Mobile Networks," EURASIP J. Wireless Comm. and Networking, vol. 2006, no. 2, p. 19, Apr. 2006.

[12] Y. Zhang, "Authentication Overhead in Wireless Networks," Proc. IEEE Int'l Conf. Comm. (ICC), May 2008.

[13] J.-A. Saraireh et al., "Analytical Model for Authentication Transmission Overhead between Entities in Mobile Networks," ELSEVIER Computer Comm., vol. 30, no. 8, pp. 1713-1720, June 2007.

[14] Y. Zhang et al., "An Improvement for Authentication Protocol in Third-Generation Wireless Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2348-2352, Sept. 2006.
[15] L.-Y. Wu et al., "Authentication Vector Management for UMTS," IEEE Trans. Wireless Comm., vol. 6, no. 11, pp. 4101-4107, Nov. 2007.
[16] Y. Zhang et al., "A Study on Evaluating Authentication Traffics in the Next Generation Wireless Networks," Proc. IEEE Int'l Conf. Comm. (ICC), June 2006.

[17] T. Fawcett, "ROC Graphs: Notes and Practical Considerations for Researchers," HP Laboratories, HPL-2003 4,http://www.hpl.hp.com/techreports/ 2003/HPL-2003-4.HTML,2013

[18]J. Cao, M. Ma, H. Li and Y. Zhang "A Survey on Security Aspects for LTE and LTE-A Networks", *IEEE Commun. Surveys Tuts.*, 2013

[19] G.M. Køien, "Mutual Entity Authentication for LTE," Proc. IEEE Seventh Int'l Wireless Comm. and Mobile Computing Conf. (IWCMC) July 2011.

[20] Chan-Kyu Han and Hyoung-Kee Choi "Security Analysis of Handover Key Management in 4G LTE/SAE Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 2, FEBRUARY 2014

[21]N.Seddigh, B.Nandy, R.Makkar, J.F.Beaumont "Security Advances and Challenges in 4G Wireless Networks," IEEE Eighth Annual International Conference on Privacy, Security and Trust, 2010.