INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

(Volume2, Issue3)

Available online at: www.Ijariit.com

Complex Key Amalgamation Method for Secure Authentication (CKAM-SA) for 4G/LTE Networks

Zinnia

CSE, GURUKUL VIDYAPEETH

Zinniaarora1@gmail.com

ABSTRACT-- It is normal that a scope of security dangers will develop in 4G remote because of various components including: Takeoff from restrictive working frameworks for hand held gadgets to open and institutionalized working frameworks open nature of the system structural planning and conventions (IP-based). With this move to open conventions and principles, 4G remote systems are currently vulnerable to PC assault methods exhibit on 70 the Internet. Such systems will be progressively powerless against a scope of security assaults including for instance Malware, Trojans and Viruses. Aside from end-client hardware posturing conventional security dangers, it is normal that new patterns, for example, SPIT (SPAM for VoIP) will likewise turn into a security concern in 4G LTE and WiMAX. Other VoIP-related security dangers are likewise conceivable; for example, SIP enrolment commandeering where the IP location of the criminal is built into the bundle header, along these lines, overwriting the right IP address. In the proposed model, the major focus has been shifted over the robust and secure authentication key mechanism for the 4G/LTE models to add the higher level to the security of the 4G/LTE networks. The complex key mechanism has been designed for the generation of the complex key to add the higher level of security to the 4G/LTE networks channels. The experimental results have justified the performance of the proposed model in the terms of time complexity, uniqueness of the keys, etc.

Keywords— AKA, Lightweight key management, LTE authentication, multi-factor authentication.

I. INTRODUCTION

Imagine a circumstance where while travelling in a vehicle in a big metropolis with a small handheld wireless device, an individual can seamlessly envision the whole environment ahead (like buildings, streets, highways, and shopping malls) and at the same time, he will track different vehicles which will are available in his technique to avoid any accidents. however at the present time wireless systems becomes want of individuals, as 4G designed that have high intelligence, user-attentive customized service like virtual navigation a reality. There are varied industries and analysis organizations worldwide like NTT DoCoMo, QualComm, Nokia, Ericsson, Motorola, Alcatel, WWRF, ITU, IEEE, Mobile VCE and 4GW-PCC, are geared up to form 4G wireless systems hit the industrial market at the start in 2010.This IPv6-based latent 4G framework, normally represented as MAGIC (mobile phone multimedia system, anytime anyplace access, international quality settle for, enclosed wireless resolution and tailored personal services), would be terribly energetic and considerably cowl the disadvantages of 3G wireless systems.

Fourth generation (4G) technology provides numerous advancements to the wireless market, plus downlink data rates well over 100 megabits per second (Mbps), low latency, very effective spectrum use and low-cost implementations. 4G developments promises to convey the wireless experience to a completely new level with spectacular user applications, for instance, it provides higher quality pictures, smart quality videos and user friendly interface. 4G additionally provides higher rate over 2G, 3G and 3.5G. Fourth generation of wireless technology has a lot of distinction when put next to earlier wireless technology like 3G and 2G. The most distinction in 4G, it

works on TCP/IP design and suite of protocols as a result of TCP/IP design (open communication protocol) has a lot of security problems as compared to 3G and 2G. 4G wireless technology permits accessing specific services that give data on demand at high speed and low price.

Key administration at the SS has been intended to protect it from replay assaults. The SS can figure out whether a Key Reply message is new or old. This is conceivable since the old TEK (Traffic Encryption Key) and new TEK are incorporated in the Key Reply message. Be that as it may, if an aggressor replays Key Request messages to the BS, it can trigger incessant trade of keying materials. This will bring about disarray at the SS and fumes assets at the BS. Another issue emerges from the blend of the TEK lifetime and crypto calculation insufficiency. The TEK lifetime can be set to a worth going between 30 minutes and 7 days. It is realized that with the DES-CBC calculation, security past 232 information hinders (every information square is 64 bits) utilizing the same TEK can be traded off. The information may be helpless if the TEK lifetime is situated to a vast quality. A third issue includes key administration in multicast and telecast administrations. 802.16e uses a typical gathering activity encryption key (GTEK) for movement encryption/unscrambling. Each multicast bunch part must know this key. The exchange of GTEK to all gatherings is telecast however encoded with the common key encryption key (SKEK). The issue of in reverse and forward mystery is not tended to. At the point when another part gets the current GTEK, it can decode every single past message that were multicast amid GTEK's lifetime. What's more, nothing in the convention keeps the SS after it abandons its gathering from getting the following GKEK (group movement encryption key).

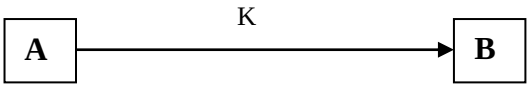
II. LITERATURE REVIEW

Seddigh et al. (2010) studied on 4G remote system security propels and its difficulties. They displayed Associate in nursing investigation of security advances and difficulties connected with new 4G remote advances and created numerous commitments to the sphere. To start out with, it targeting the protection benchmarks .Second, security-related standards, design and description for the LTE and WI-MAX advances were analysed. Anand et al. (2011) ascertained a security weakness that would direct to service disruption in 3GPP advanced LTE and HSPA+ networks as a results of recently projected channel aggregation or bonding .They were given Associate in Nursing experimental results to stimulate the matter and given analysis to see the transmit power of the malicious assailant on all the channels to form important service disruption whereas exploitation minimum power. Xiehua and Yongjun (2011) ascertained the third generation partnership(3GPP) customary was developing system design evolution (SAE)/Long term evolution (LTE) design for next generation mobile communication system. Within the LTE/SAE design, EPS-AKA (evolved packet system authentication and key agreement) procedure was wont to offer mutual authentication between the patron and also the network. Abed et al. (2012) this paper proposed has given an impression of the advancement of LTE towards Release 10. A portion of the key segments: key highlights, E-UTRAN, EPC, client plane convention and control plane convention stack are portrayed here. Likewise, it gave a standpoint of the development of LTE toward LTE-Advanced as well as full IMT-Advanced capacities that were finished. Alezabi et al. (2014) planned a productive EPS-AKA (EEPS-AKA) convention to beat vulnerabilities, for instance, divulgement of consumer identity, procedure overhead and man-in the - centre attack (MITM) and authentication. The consumer temperament may be uncovered once man-in the centre assault has sent clear content in initial association, which prompts client character attack. Mohapatra et al. (2015) Studied of recent advances in wireless network security issues such as Physical layer issues, Wi-Max Mac layer issues, QoS problems and 4G Wi-Fi security problems. It created a many contribution to the wireless networking field. First, it studied the 4G mail threats, risk and their style choices.

III. EXPERIMENTAL DESIGN

The proposed model has been designed to protect the 4G/LTE (Long term evolution) model during the initial setup phase as well as the post-setup phase. The proposed model key model utilizes the double layer encryption to ensure the security of the keys during the transmission. The advance encryption standard (AES) has been used along with the RSA (Ron Rivest, Adi Shamir and Leonard Aldeman) algorithm to prevent the key model from the active or passive attacks. The highest threat is caused by the passive attacks, such as replication attacks, replay attacks or session hijacking attacks, which are used to steal the information from the communication channel. The proposed key model has been designed as the point-to-point centrally managed key scheme. The proposed model works in the server-client model, where the BTS plays the role of server and the mobile stations connects as the client in the communication model.

(a)Point To Point Key Distribution:



(b)Key Distribution Center:

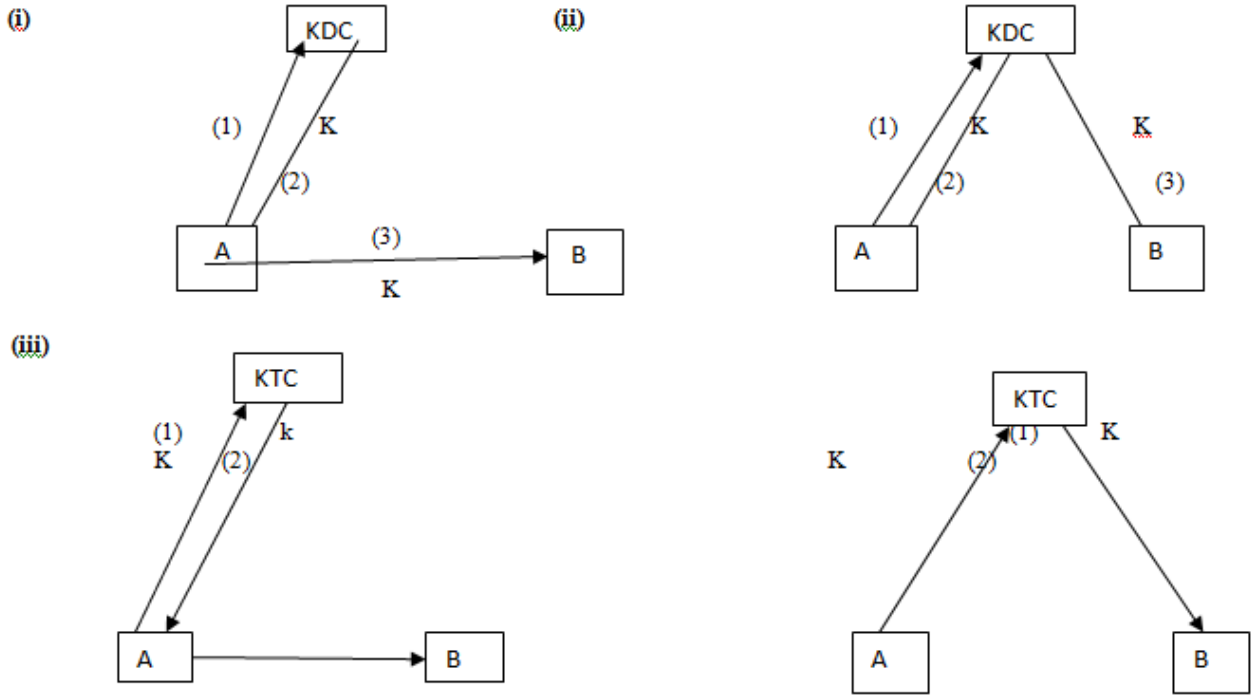


Figure 3.1: The key management scenarios

Point-to-Point mechanism: These involve two parties communicating directly (see §12.3.1). 2. Key distribution centres (KDCs). KDCs are used to distribute keys between users which share distinct keys with the KDC, but not with each other. A basic KDC protocol proceeds as follows.1 Upon request from A to share a key with B, the KDC T generates or otherwise acquires a key K, then sends it encrypted under KAT to A, along with a copy of K (for B) encrypted under KBT . Alternatively, T may communicate K (secured under KBT) to B directly. 3. Key translation centers (KTCs). The assumptions and objectives of KTCs are as for KDCs above, but here one of the parties (e.g., A) supplies the session key rather than the trusted center. A basic KTC protocol proceeds as follows.2 a sends a key K to the KTCT encrypted under KAT. The KTC deciphers and re-enciphers K under KBT, then returns this to A (to relay to B) or sends it to B directly. KDCs provide centralized key generation, while KTCs allow distributed key generation. Both are centralized techniques in that they involve an on-line trusted server. The Point-to-point and centralized key management, Point-to-point communications and centralized key management using key distribution centers or key translation centers, are examples of simple key distribution (communications) models relevant to symmetric-key systems. Here “simple” implies involving at most one third party nodes. These are illustrated in Figure 3.1 and described below, where KXY denotes a symmetric key shared by X and Y.

Algorithm 3: Key Scheme Algorithm Sequence for Function Calling

1. The 4G cell unit (4GCU) receives the request for call to the user in its region
2. It notifies the concerned user’s station (UST) and asks for its availability
3. If the UST is available and ready, then the connection setup phase is initialized
4. The UST is asked to return the pre-shared information.
5. UST provides the pre-shared information entities to the 4GCU.
6. If the pre-shared information phase is completed successfully
7. The communication takes place between the 4GCU and the UST and the call is forwarded
8. The key table is shared between the 4GCU and UST.
9. Otherwise the communication request is rejected and the call is dropped
10. If step 7 is true the timer is initialized with the given span
11. Once the timer is expired
    a. The 4GCU prepares the query key by using the complex mechanism
    b. Dual-encrypt the key using the AES and RSA
    c. Forward the key to the UST
    d. UST decrypts the key and perform the complex table lookup
    e. UST finds the paired key and return with the complex reply key to the 4GCU.
    f. 4GCU verifies the match

g. The communication keep running if the verification is successful
h. And fails otherwise
i. The timer is restarted from the beginning

12. When the timer expires again go to 11

IV. RESULT ANALYSIS

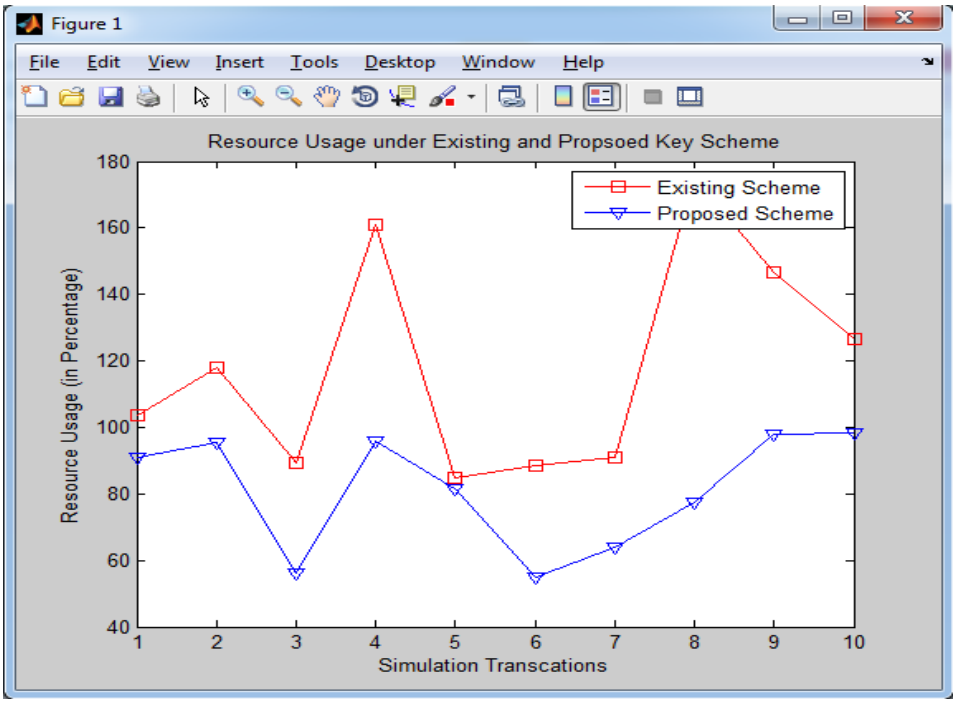


Figure 1: Resource Usage based comparative analysis

The performance of the proposed model has been observed on the basis of resource usage with the existing model implementation. The proposed model has been classified better than the existing model as it has scored lower levels of resource usage for the similar levels of attacks data over the LTE networks. The proposed model has controlled data attack data during the attack hours effectively and kept the resource usage under the limit of 100%, whereas the existing system has been found processing the large volumes of data than their capacity.

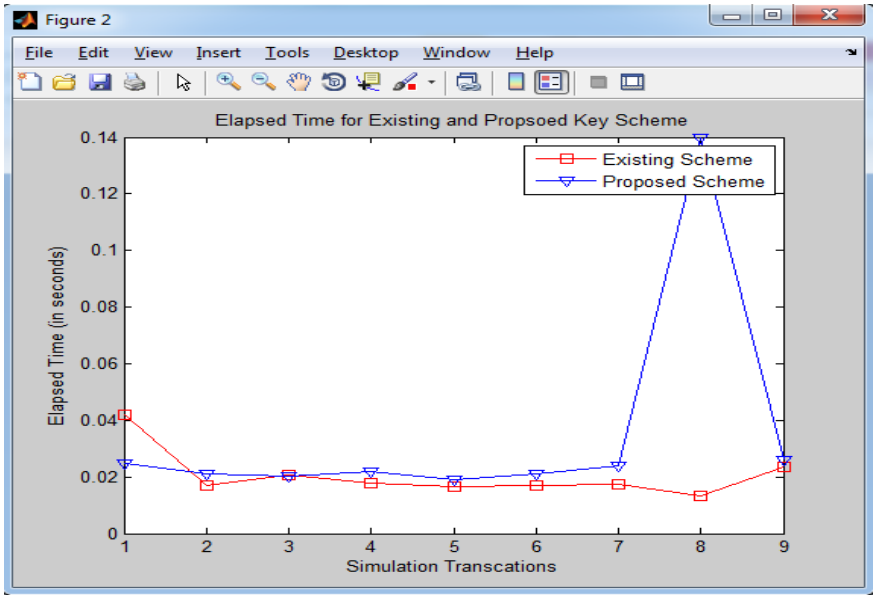


Figure 2: Elapsed Time based comparative analysis between the proposed and existing model

The elapsed time has been recorded for the key transfer and key verification transactions. The proposed model has been found better than the existing model as it has taken less time for the key management process. The proposed model is quicker than the existing model for the key exchange and verification transactions. The detailed results for elapsed time can be seen in the following table:

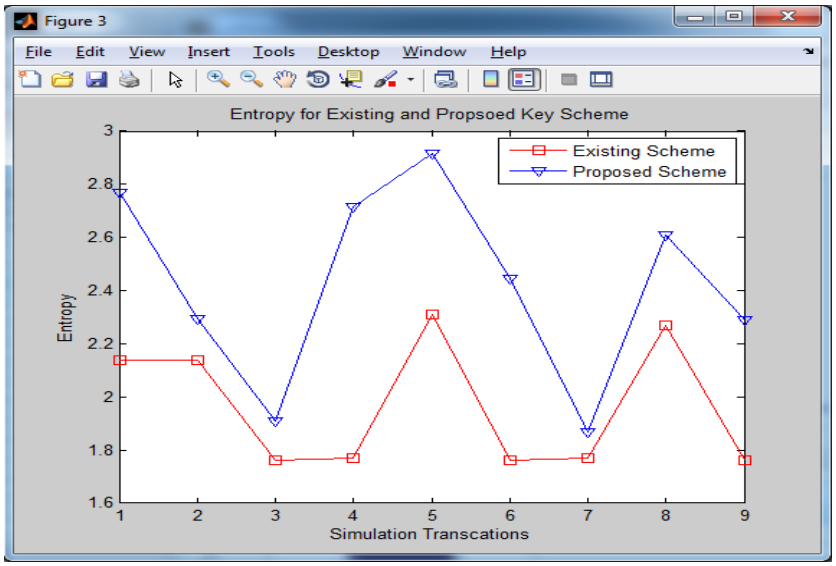


Figure 3: Entropy evaluated based key data uniqueness evaluation between the proposed and existing models

The entropy gives the uniqueness of the keys being exchanged during the communication. The entropy has been found higher in the case of the proposed model which shows the proposed model effectiveness in the case of uniqueness of the keys in the key table.

V. CONCLUSIONS

The comparative analysis has been performed over all of the five simulation scenarios between existing and proposed model. The performance evaluation has been performed on the basis of resource usage, elapsed time and entropy. The proposed model has been proved itself as the best model than the existing model. The proposed model has been proved to efficient than the existing model on the basis of all three performance parameters. The proposed model results have recorded with the highly vital values in comparison with the existing model of the 4G/LTE security. The proposed model can be considered as the clear winner when analyzed from the input comparison in the results section. In the future the more robust and quick response authentication method can be produced by using the smart key generation with the small but complex data computations to achieve the stronger security level. Also the smart security based intensity mechanism can be proposed, which analyzes the level of threat before imposing the security over the given link.

REFERENCES

1. Seddigh N., Nandy B., Makkar R. and Beaumont J.F. (2010) "*Security advances and challenges in 4G wireless networks.*" In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference IEEE, pp. 62-71.
2. Anand S., Hong k., Sengupta S., Chandramouli R. and Subbalakshmi K. P. (2011) "*Security Vulnerability due to channel aggregation/bonding in LTE and HSPA+ networks*" accepted in IEEE global communications conference (GLOBECOM).
3. Xiehua L. and Yongjun W. (2011) "*Security enhanced authentication and key agreement protocol for LTE/SAE network"* Published in wireless communication, networking and mobile company (WiCOM), 7th international conference on IEEE, pp. 1-4.
4. Alezabi, Ali K., Hashim F., Hashim S. J. and Ali B.M. (2014) "*An efficient authentication and key agreement protocol for 4G (LTE) networks*." In Region 10 Symposium, 2014 IEEE, pp. 502-507.
5. Mohapatra S. K., Swain B., Das P. (2015) "*Comprehensive survey of possible security issues on 4G networks"* IJNSA, vol. 7, No. 2, pp. 61-69.
6. Mohapatra S. K., Swain B., Das P. (2015) "*Comprehensive survey of possible security issues on 4G networks"* IJNSA, vol. 7, No. 2, pp. 61-69.
7. Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "*An overview of image steganography.*" *ISSA*. 2005.
8. Morshed M. M. and Islam M.R. (2013) *"CBSRP: Cluster Based Secure Routing Protocol",* IACC, vol. 3, IEEE, pp. 571-576.
9. Muhammad Asad, Junaid Gilani, Adnan Khalid "An *Enhanced Least Significant Bit Modification Technique for Audio Steganography*", international conference on Computer Networks and Information Technology (ICCNIT), vol. 1, pages 143-147, IEEE, 2011.
10. Navita Aggarwal, Himanshu Sharma "*An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography*", IJCSMC, vol. 2 issue 5,pp. 376-385, May 2013.

11. N. Suganthi, V. Sumathy, "*Energy Efficient Key Management Scheme for Wireless Sensor Networks*", vol 9, issue 1, pp. 71-78, INT J COMPUT COMMUN, 2014.
12. Purkhiabani M., Salahi A. (2012) "*Enhanced Authentication and key agreement procedure of next generation 3GPP Mobile networks"* International journal of information and electronic engineering, vol. 2, No. 1, pp. 69-77.
13. Rakesh, S., et al. "*Image encryption using block based uniform scrambling and chaotic logistic mapping.*" International Journal on Cryptography and Information Security 2.1 (2012): 49-57.
14. Rivero, Cristobal, and Prabhat Mishra. Lossless Audio Compression: A Case Study. Technical Report 08-415, Department of computer and information Science and Engineering, University of Florida, Gainesville, FL32611, USA, 2008.
15. Salama, Diaa, Hatem Abdual Kader, and Mohiy Hadhoud. "*Studying the Effects of Most Common Encryption Algorithms*." International Arab Journal of e-Technology 2.1 (2011): 1-10.
16. Sasan Adibi, A low overhead scaled equalized harmonic-based voice authentication system, Telematics and Informatics, vol. 31, pp. 137-152, Science Direct, 2013.

