AUSTRALIAN JOURNAL OF BASIC AND APPLIED SCIENCES

ISSN:1991-8178 EISSN: 2309-8414
Journal home page: www.ajbasweb.com

Multifactor Complex Key based Authorization and Key Authentication (MCK-AKA) for Efficient LTE Networks

[1]Kanica and [2]Dr. Anuj Kumar Gupta

[1, 2]Dept. of Computer Science and Engineering, CGC - COE Punjab, India

Address For Correspondence:
Kanicam Student Dept. of Computer Science and Engineering, CGC - COE Punjab, India.
E-mail: kanicasept1991@gmail.com

ARTICLE INFO

Article history:
Received 18 February 2017
Accepted 15 May 2017
Available online 18 May 2017

Keywords:
Introduction to 4G, 4G Standards, Security issues, Result Analysis.

ABSTRACT

Background: The 4G/LTE networks are the popularly growing cellular networks, and the large numbers of subscribers are joining the 4G networks. The 4G/LTE networks offer the higher bandwidth at more than 100 Mbps for the transmission of the data among the given network. 4G developments promises to convey the wireless experience to a completely new level with spectacular user applications. **Objective:** 4G/LTE network is evaluated for voice data in terms of efficiency. **Results:** The results obtained from the proposed model simulation has been deeply analyzed and compared against the other schemes in order to evaluated the effectiveness of the proposed model. The efficiency of the proposed model has been evaluated for the voice data channelized over the 4G/LTE channels for the given simulation environment. **Conclusion:** The performance parameters of the projected resource and data overhead has been evaluated as the primary analysis factors which elaborates the performance of the proposed scheme in the terms of security and network performance.

INTRODUCTION

Introduction to 4G:

LTE (Long Term Evaluation) is a 4G technology developed for GSM network. It is the first 4G technology used in mobile phones across the world and was proposed by Docomo. It is a high speed data transfer for mobile phones with 299.6 Mbps download speed and 75.4 Mbps upload speed. (Abed, G.A., *et al*., 2012; Alezabi, *et al*., 2014).

This era marked the beginning of full-fledged huge revenue generating multimedia Internet applications and e-commerce. (Anand, S., *et al*., 2011) However, with the huge worldwide increase in the number of mobile users each day and with emerging demands like totally user-centric services, high speed streaming Internet multimedia services, seamless global roaming with ubiquitous coverage and unhampered QoS support, 3G systems have started showing their limitations with bandwidth availability, (Cao, *et al*., 2015) spectrum allocation, air interference standards and lack of seamless transport mechanisms between different networks. Moreover, different short range communication systems like WLAN, Bluetooth and HIPERLAN as well as broadcast communication systems with different features spanned during this time each with its own merits and demerits targeting different types of users and different service types making the situation more complicated for 3G systems. (Cao, *et al*., 2015; Cao, *et al*., 2015; Chandramouli, R., *et al*., 2013).

To Cite This Article: Kanica and Dr. Anuj Kumar Gupta., Multifactor Complex Key based Authorization and Key Authentication (MCK-AKA) for Efficient LTE Networks. ***Aust. J. Basic & Appl. Sci.,*** *11(8): 20-27, 2017*

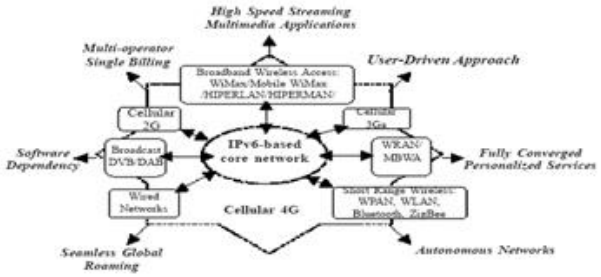

Fig. 1.1: Cellular 4G

Technology Used In 4G:

The two types of technologies used in 4G are:-

1. OFDM (Orthogonal Frequency Division Multiplexing):- The main reason 4G is faster than 3G is because of OFDM. It sounds complicated but it's the same technology used in Wi – Fi, digital TV and radio. (Cunningham, Stuart, *et al*., 2005) It is a technique for squeezing more data onto the same amount of radio frequency. In this technology data is split up and send via small chunks of frequency in parallel, therefore increasing the capacity of network. (Damgard, I., *et al*., 2013; Gary, C., Kessler, 2014)

2. MIMO (Multiple Input Multiple Output):- MIMO is the reason 4G is able to provide faster speeds. (Huang, J., *et al*., 2013) It allows more data to be transferred without requiring additional bandwidth or drawing more power. MIMO is found in more smartphones and some tablets. (IngYannSoon, *et al*., 2012).

4g Wireless Standards:

4G principally works on two standards and these are:

Wi-MaX:

It stands for Worldwide Interoperability for Microwave Access, and is a wireless communication standard. (Jalal Karam, 2008) It was developed in 2001 and borrowed some of its technology from a service known as WiBRO, used in South Korea .It operates using many of the same fundamental principles as Wi – Fi networks, it offers a greater signal range than the 100 feet provided by the most conventional Wi-Fi modems. (Khalifa *et al*., 2008; Liebchen, Tilman, *et al*., 2005) It was initially designed to provide 30 to 40 megabit –per second data rates, with the 2011 update providing up to 1/Gbit /s for fixed stations. (Mazieres, D., et qal., 1999)

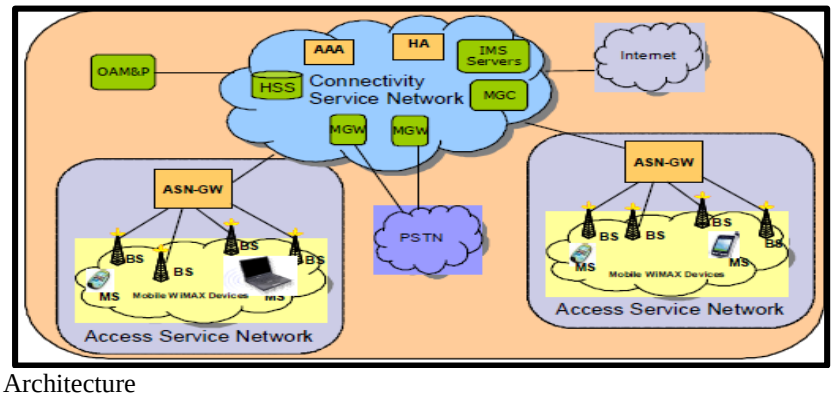

Fig. 1.2: Wi- MaX Architecture

LTE (Long Term Evolution):

It is a standard for high speed wireless communication for mobile phones and data terminals based on GSM/EDGE/UMTS/HSPA.It increases the capacity and speed using a different radio interface together with core network improvements It is commonly marketed as 4G LTE ,but it does not meet the technical criteria of a 4G wireless service. (Milind Mathur, Ayush Kesarwani, 2013)

LTE Architecture:

The network architecture of LTE is comprised of following three main components:-

i) UE (User Equipment):

The internal architecture of the user equipment for LTE is identical to one used by UMTS and GSM. It handles all the communication functions. It terminates data streams. It runs an application known as Universal Subscriber Identity Module (USIM). (Mohammadi, S., H. Abbasimehr, 2010)

ii) E- UTRAN(The Evolved UMTS Terrestial Radio Access Network):

It handles the radio communications between the mobile and the evolved packet core and just has one component ,the evolved base stations ,called eNode or eNb. Each eNB is a base station that controls the mobiles in one or more cells. (Mohapatra, S.K., *et al*., 2015; Morkel, *et al*., 2005). The base station that is communicating with a mobile is known as its serving eNB. (Morshed, M.M. and M.R. Islam, 2013)

iii) EPC (Evolved Packet Core):

It communicates with packet data networks in the outside world such as the internet, private corporate networks or the IP multimedia system. (Muhammad Asad, *et al*., 2011)

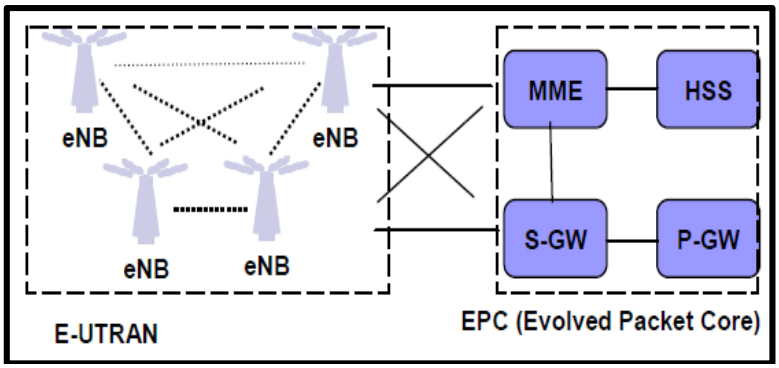

Fig. 1.3: LTE architecture

Literature Survey:

Bulakci *et al*. (2010) ascertained a Relaying that was capable sweetening to current radio access networks. Seddigh *et al*. (2010) studied on 4G remote system security propels and its difficulties. 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. Purkhiabani and Salahi(2012) They characterized new verification convention to determined and uncertain security and movement issues for 3GPP SAE AKA and enhanced proposed-AKA instrument and its investigation contrasted with EPS-AKA to enhance execution of confirmation convention inventiveness in the LTE system and better administration the validation flagging activity overhead, another proposed verification convention was recommended to determine a few deformities, for example, AKA processing in HSS and data transfer capacity utilization. Shah *et al*.(2012) They was represented the uses of 4G innovation considering the importance of fixing to 4G frameworks as a superior administration contrasted with the 3G technology. Chandramouli *et al*. (2013) worked on Cryptographic Key ManagementIssues & Challenges in Cloud Services. Damgard *et al*.(2013) planned a secure key management methodology for cloud environments. Authors have studied the amount of security on the idea what they will and what they can't get within the security models.

Experimental Design:

The existing model is based upon the evolved packet system authentication and key agreement (EPS-AKA) and has been improved as the efficient EPS-AKA (also EEPS-AKA). The EEPS-AKA model has been comprised of the security model to protect against the information disclosure vulnerabilities and man in the middle attack. The existing system is two-column based key management authentication model with the elliptic curve cryptography. The existing model has been made to share four messages for one round of authentication. It utilizes the simple password exponential key exchange (SPEKE) model of the base model implementation and has been developed with certain defined improvements.

The proposed model has been offered to protect the voice data and user data in the 4G environments. The key scheme has been designed to be used on the point-to-point architecture using the centralized base transceiver station (BTS) node. The 4G base station ensures its security by using the authentication scheme between the mobile nodes and base station. The proposed model scheme has been enlisted as following:

For authentication purpose, we are using a table with 5 columns and multiple rows in which the first 3 columns (i.e. a, b, c) are used for query key generation and the last 2 columns (i.e. d, e) are used for reply key building. The table is shown below:

Table 3.1: Key Table

A	B	C	d	e

Query key generation:

Query key= round(log10(sin(a)*cos(b)*tan(c))*887000+(a*b*c))

Reply key generation:

Reply key= round(log10(sin(d), atan2(d,e)*180/pi)*347100)

Main Key Generation Policy:

Algorithm: Key Scheme Algorithm Sequence for Function Calling:

CASE 1: When mobile node calls out:

1. Mobile node initializes the call setup phase, and request 4G base station to complete the call.
2. The 4G base station initializes the authentication process. CASE 2: When base station receives the call for mobile node:
1. The 4G base station receives the call for the mobile node.
2. The 4G base station requests the mobile station and verifies the ready state.
3. When mobile node replies with the ready state, 4G base station initializes the authentication process. MAIN

Algorithm:

1. The 4G base station infuses the multi-column keys to prepare the query key.
2. The query key is encrypted using the ECC algorithm.
3. The query key is forwarded to the mobile station.
4. The mobile station prepares the reply key by verifying the query key column data and marks the reply key rows.
5. The reply key is prepared by infusing the multiple keys information in the marked columns.
6. The reply key is encrypted using the ECC algorithm.
7. The reply key is forwarded towards the 4G base station.
8. The 4G base station verifies the query key against the reply and prepares the decision.
9. If the verification decision is successful
10. The call setup is complete and call is forwarded to the target mobile station.
11. Time counter (Tc) is initialized
12. Else
13. The call is dropped and the mobile node is informed about the authentication failure.
14. When the timer (Tc) expires, the exchange process is repeated.
15. If key verification is successful
16. The channel stays intact
17. Otherwise
18. The call is terminated

Result Analysis:

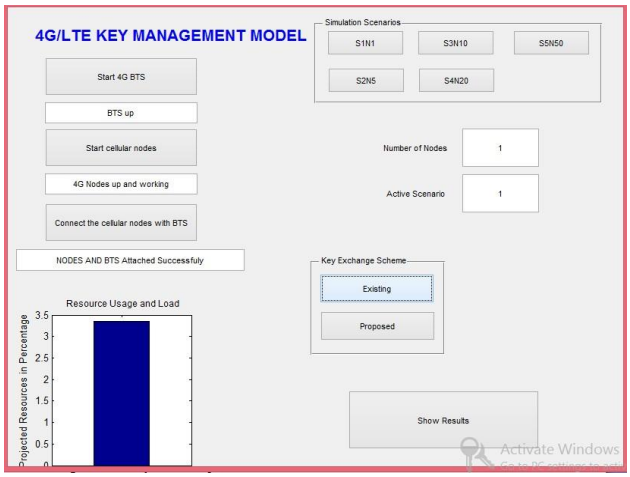

Fig. 4.1: The system UI Snapshot for the working system

Project resources: The projected resource has been evaluated for the measurement of the utilization of the resources over the given 4G/LTE cellular network environment in the proposed model simulation. The high performance is indicated by the lower value of the projected resources computed from the simulation environment and higher value indicates the lower performance. MCK-AKA has been considered better than EEPS-AKA as it has been measured with the lower value for projected resources over the given simulation scenario of LTE network. The detailed result evaluation has been described below**:**

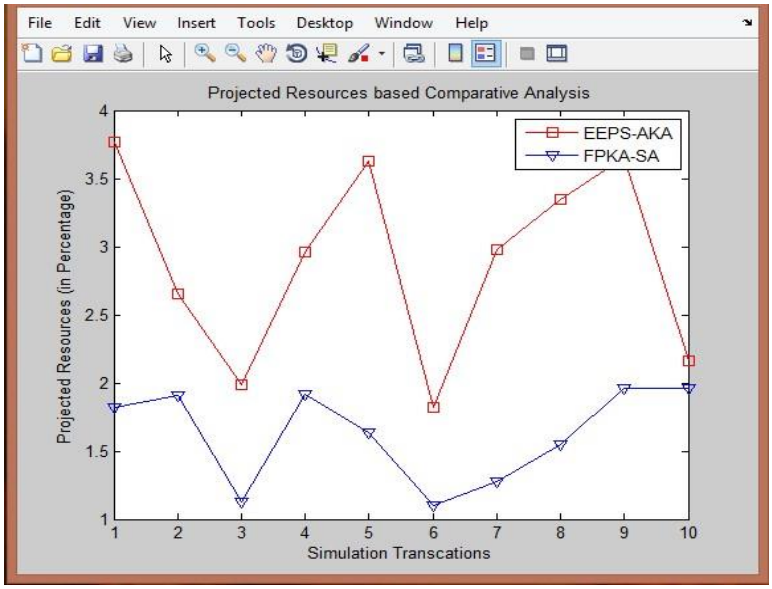

Fig. 4.2: Projected resources based graph for scenario 1

Entropy: The key efficiency, size of population and the uniqueness of the entities in the given key table is measured by using the entropy parameter. The unique data decreases the risk of key exposure to the hacking attempts, which has been strongly observed from the proposed model simulation. The consistently high entropy justifies the strength of the security of the 4G/LTE networks. The detailed results for entropy can be seen below:

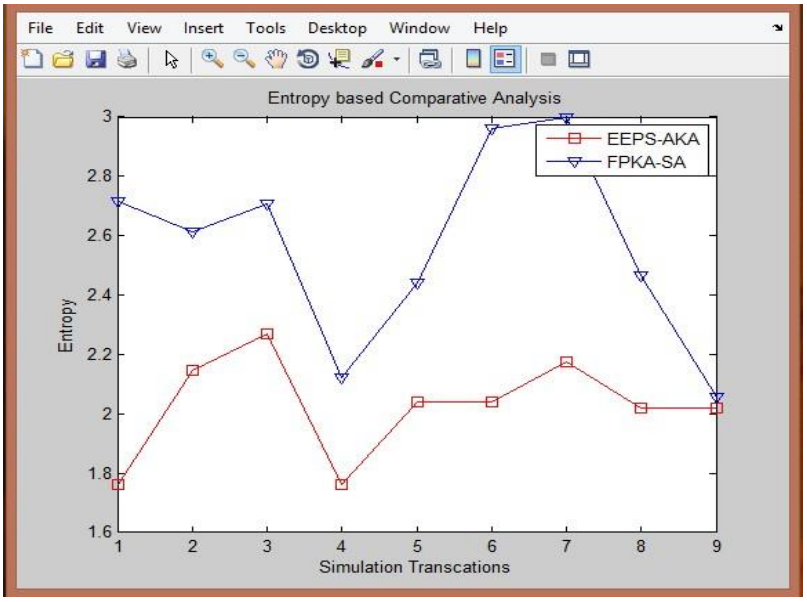

Fig. 4.3: Entropy based graph for scenario 1

The comparison of the evaluated results has been performed over the results obtained from the existing and proposed models. The performance evaluation has been performed on the basis of projected resources and entropy. MCK- AKA has been proved itself as the better model than EEPS-AKA. MCK-AKA has been proved to be efficient than EEPS-AKA on the basis of both the performance parameters.

Table 4.1: Projected Resources based comparison for scenario 1

Key Index	EEPS-AKA	MCK-AKA
1	3.7667	1.8164
2	2.6499	1.9063
3	1.9840	1.1250
4	2.9604	1.9141
5	3.6282	1.6328
6	1.8221	1.0977
7	2.9796	1.2773
8	3.3467	1.5469
9	2.1651	1.9648

Table 4.2: Entropy based comparison for scenario 1

	EEPS-AKA	MCK-AKA
1	1.7632	2.7158
2	2.1466	2.6115
3	2.2706	2.7054
4	1.7632	2.1222
5	2.0412	2.4402
6	2.0412	2.9598
7	2.1762	2.9963
8	2.0207	2.4678
9	2.0207	2.0544

Conclusion:

The proposed model named MCK-AKA has been compared against the existing model of EEPS-AKA over the standard 4G/LTE simulation scenario with similar structure and environment. The detailed analysis of the simulation results has been conducted by analyzing the results obtained from the existing and proposed model simulations. The proposed model of MCK-AKA has been described efficient and effective while evaluated on the basis of the projected resources and entropy for the coalition of the network load and uniqueness respectively. Minimum of the 10 percent improvement has been observed in the favor of the proposed model when compared on the basis of various performance parameters in the variety of simulation scenarios. The attack situations have been analyzed theoretically and the effective in the results has been observed in the proposed model to mitigate t he security threats with the new security model than the existing model. The appropriate future enhancement of the proposed model may lies in the enhancement of the message level encryption for the insurance of the data security. The performance evaluation of the proposed model can be determined in the various aspects, scenarios and network platforms.

REFERENCES

Abed, G.A., M. Ismail and K. Jumari, 2012. “The Evolution to 4G Cellular Systems: Architecture and Key Features of LTE-Advanced Networks” IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), 2(1): 21-26.

Alezabi, Ali K., F. Hashim, S.J. Hashim and B.M. Ali, 2014. "An efficient authentication and key agreement protocol for 4G (LTE) networks." In Region 10 Symposium, IEEE, pp: 502-507.

Anand, S., k. Hong, S. Sengupta, R. Chandramouli and K.P. Subbalakshmi, 2011. “Security Vulnerability due to channel aggregation/bonding in LTE and HSPA+ networks” accepted in IEEE global communications conference (GLOBECOM).

Bulakci, O., A.B. Saleh, S. Redana, B. Raaf and j. Hamalainen, 2010. “ Enhanced LTE-advanced Relay deployment via Relay cell Extension” presented at the 15th international OFDM-Workshop (InOWo 10).

Cao, Jin, Hui Li, and Maode Ma, 2015. "GAHAP: A group-based anonymity handover authentication protocol for MTC in LTE-A networks." In Communications (ICC), 2015 IEEE International Conference on, pp: 3020-3025.

Cao, Jin, Hui Li, Maode Ma, and Fenghua Li, 2015. "UGHA: Uniform group-based handover authentication for MTC within E-UTRAN in LTE-A networks." In Communications (ICC), 2015 IEEE International Conference on, pp: 7246-7251.

Cao, Jin, Maode Ma, and Hui Li, 2015. "GBAAM: group-based access authentication for MTC in LTE networks." Security and Communication Networks.

Chandramouli, R., M. Iorga and S. Chokhani, 2013. “Cryptographic Key Management Issues & Challenges in Cloud Services”, Computer Security Division Information Technology Laboratory, NIST.

Cunningham, Stuart, Vic Grout and John McGinn, 2005. "Play it Again, Babbage!–A Framework to Exploit Musical Repetition for High-Quality Audio Compression."Proceedings of IADIS-International Conference on WWW/Internet, Lisbon, Portugal, 19th-22nd.

Damgard, I., T.P. Jakobsen, J.B. Nielsen and J.I. Pagter, 2013. “Secure Key Management in sthe Cloud”, Cryptography and Coding Lecture Notes in Computer Science, 8306: 270-289.

Gary, C., Kessler, 2014. “An Overview of Cryptography: Cryptographic”, HLAN, 1.

Huang, J., F. Qian, Y. Guo, Y. Zhou, Q. Xu, Z.M. Mao, S. Sen and O. Spatscheck, 2013. “An in-depth study of LTE: Effect of network protocol and application behavior on performance” Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM, pp: 363-374.

IngYannSoon, FengZhou, ZhenLi, HaijunLei, Baiying Lei, 2012. A robust audio watermarking scheme based on lifting wavelet transform and singular value decomposition, Signal Processing, 92: 1985-2001.

Jalal Karam, 2008. “A New Approach In Wavelet Based Speech Compression”, Mathematical Methods, Computational Techniques, Non-Linear Systems, Intelligent Systems, pp: 228-233.

Khalifa, Othman O., Sering Habib Harding and Aisha-Hassan A. Hashim, 2008. "Compression using Wavelet Transform." Signal Processing: An International Journal (SPIJ) 2.5: 17-26.

Liebchen, Tilman, *et al*., 2005. "The MPEG-4 audio lossless coding (ALS) standard-Technology and applications." AES 119th Convention.

Mazieres, D., M. Kaminsky, M.F. Kaashoek and E. Witch, 1999. “Separating key management from file system security” Published as operating Systems Review, 17th ACM Symposium on Operating systems principles (SOS 99), pp: 124-139.

Milind Mathur, Ayush Kesarwani, 2013. “Comparison between DES, 3DES, RC2, RC6, BLOWFISH and AES”, NCNHIT, 1: 143-148

Mohammadi, S., H. Abbasimehr, 2010. “A high level security mechanism for internet polls”, ICSPS, 3: 101-105.

Mohapatra, S.K., B. Swain, P. Das, 2015. “Comprehensive survey of possible security issues on 4G networks” IJNSA, 7(2): 61-69.

Morkel, Tayana, Jan HP Eloff and Martin S. Olivier, 2005. "An overview of image steganography." ISSA.

Morshed, M.M. and M.R. Islam, 2013. “CBSRP: Cluster Based Secure Routing Protocol”, IACC, vol. 3, IEEE, pp: 571-576.

Muhammad Asad, Junaid Gilani, Adnan Khalid, 2011. “An Enhanced Least Significant Bit Modification Technique for Audio Steganography”, international conference on Computer Networks and Information Technology (ICCNIT), 1: 143-147.

Suganthi, N., V. Sumathy, 2014. “Energy Efficient Key Management Scheme for Wireless Sensor Networks”, 9(1): 71-78, INT J COMPUT COMMUN.

Navita Aggarwal, Himanshu Sharma, 2013. “An Efficient Pixel-shuffling Based Approach to Simultaneously Perform Image Compression, Encryption and Steganography”, IJCSMC, 2(5): 376-385.

Purkhiabani, M., A. Salahi, 2012. “Enhanced Authentication and key agreement procedure of next generation 3GPP Mobile networks” International journal of information and electronic engineering, 2(1): 69-77.

Rakesh, S., *et al*., 2012. "Image encryption using block based uniform scrambling and chaotic logistic mapping." International Journal on Cryptography and Information Security, 2.1: 49-57.

Rivero, Cristobal and Prabhat Mishra, 2008. Lossless Audio Compression: A Case Study. Technical Report 08-415, Department of computer and information Science and Engineering, University of Florida, Gainesville, FL32611, USA.

Salama, Diaa, Hatem Abdual Kader and Mohiy Hadhoud, 2011. "Studying the Effects of Most Common Encryption Algorithms." International Arab Journal of e-Technology, 2.1: 1-10.

Sasan Adibi, 2013. A low overhead scaled equalized harmonic-based voice authentication system, Telematics and Informatics, 31: 137-152.

Seddigh, N., B. Nandy, R. Makkar and J.F. Beaumont, 2010. “Security advances and challenges in 4G wireless networks." In Privacy Security and Trust (PST), 2010 Eighth Annual International Conference IEEE, pp: 62-71.

Shah, I., S. Shukla, R. Shrotriya, N. Mehta, N. Mehta and S. Bakliwal, 2012. “Comparative Study of 4G Technology, Application and Compatibility in Prevailing Networks” IJECCT, 2(6): 287-291.

Singh, N., M.S. Saini, 2015. “Performance evaluation of secure Asymmetric Key Exchange Mechanism for 4G networks” International journal of computer applications, 118(23): 10-15.

Sonja Grgic, Mislav Grgic, 2001. “Performance Analysis of Image Compression Using Wavelets”, ITIE, 48(3): 682-695.

Taqa, Alaa, A., A. Zaidan and B.B. Zaidan, 2009. "New framework for high secure data hidden in the MPEG using AES encryption algorithm." International Journal of Computer and Electrical Engineering (IJCEE) 1.5: 566-571.

Tiloca, M., D.D. Guglielmo, G. Dini and G. Anastasi, 2013. “SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks”, ETFA, 18: 1-8.

Verma, O.P., R. Agarwal, D. Dafouti, 2011. “Performance analysis of data encryption algorithms”, ICECT, 5: 399-403.

Wang, J., Z. Zhang, Y. Ren, Li Bin and Kim J-u, 2014. "Issues toward networks architecture security for LTE and LTE-A networks" International journal of security and its applications, 8(4): 17-24.

Xiangui Kang, Jiwu Huang, 2003. "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression", ITCSVT, 13(8): 776-786.

Xiehua, L. and W. Yongjun, 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.

Zhang, M. and Y. Fang, 2005. "Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol", IEEE Transactions on Wireless Communications, 4(2): 734-742.

Zongwei Zhou, Jun Han, Yue-Hsun Lin, Adrian Perrig, Virgil Gligor, 2013. "KISS: Key it Simple and Secure Corporate Key Management", Trust and Trustworthy Computing Lecture Notes in Computer Science, 7904: 1-18.

Dr. Anuj Kumar Gupta; Kanica, 2016. "Areview on multilayer security architectures/models for 4G/LTE networks" IJLTET.

Dr. Anuj Kumar Gupta, Kanica**"**N-Column Authentication Key Building with Multi-Round Cryptography for High Level of Security in 4G networks."IJIET-21791.