iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42666

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

Survey on Vulnerability of 4G/LTE Network Security and Improvements

Dr. Tudi Premchander
Associate Professor, ISL Engineering College, Hyderabad, India.

Abstract: ***Network security is viewed as a huge issue in our regular routine because of its going into many individuals' exercises like social movement, showcasing and business. Notwithstanding, the requirement for a safe and strong organization has expanded. The requirements for a secure organization have expanded because of the expanding dangers and programmers in our regular routine. In view of the ongoing insights, each second the quantity of supporters is expanding multiple times around the world which refers to the quick development of 4G/LTE organizations.***
It is seen that 80% of individuals universally have claimed 4G cell phones and the number is expanding during the new quite a long while. Besides, 4G/LTE is the groundwork of the 5G network, so high level security is required. From this point, this paper presents an overview of the enhancements that have been done as of late on 4G/LTE security and uncovers the shortcomings that still exist and that will permit specialists to concentrate and work on these shortcomings.
Keywords: Attacks, 4G/LTE, vulnerability and security.

I. INTRODUCTION

The evolvements of fourth era cell network is state-of-the-art news these days. The pattern toward creating and getting more dependable and legitimate device is expanding step by step. Subsequently, the specialists commit their time researching and finding the answer for any backhaul or issue which actually exists as of not long ago in the fourth era of versatile correspondence. In light of (Ahlwat, 2018), the development from single confirmation in the original to the shared verification in the 4G/LTE networks has made the organization inclined to new sorts of dangers and weaknesses. The plan of LTE is appropriate for the requests of client for getting quick admittance to information, less postponement, high throughputs and high information rates. This large number of highlights persuade specialists to researches more and attempts to improve and safeguard LTE security from any gatecrasher. Along these lines, this exploration overviews the new enhancements and improvements on LTE security as well as sorting out the weaknesses that actually exist in the LTE organization and have to recuperate.

II. LTE AND LTE-A SECURITY DESIGN

The plan of LTE and LTE-An organization comprises of two fundamental parts, The first is Evolved Universal Terrestrial Radio Access organization (E-UTRAN) and the second is Evolved Packet Core (EPC).Only a couple of overviews have been done to help LTE security and show the potential dangers and ongoing improvement in LTE security. Be that as it may, LTE security framework engineering comprises of five layers which are characterized by the Third Generation Partnership Project (3GPP):

1) Network Access Security: Responsible for tying down the entrance of the versatile clients to the organization and ensuring the radio access interface is gotten from any assault.
2) Network Domain Security: ensures that convenient backhaul center points to securely exchange flagging data and client data at the adaptable backhaul frameworks and gets against attacks on wireline association.
3) Client Domain Security: Safe admittance to the versatile station.
4) Application space security: This licenses applications from the client and organization contemplates safely exchanging information.
5) Perceivability and Configuration of safety: Permits clients to utilize information around enabled security features and course of action of organizations. The layers are displayed in Figure 1(Liyanage et al., 2015).

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

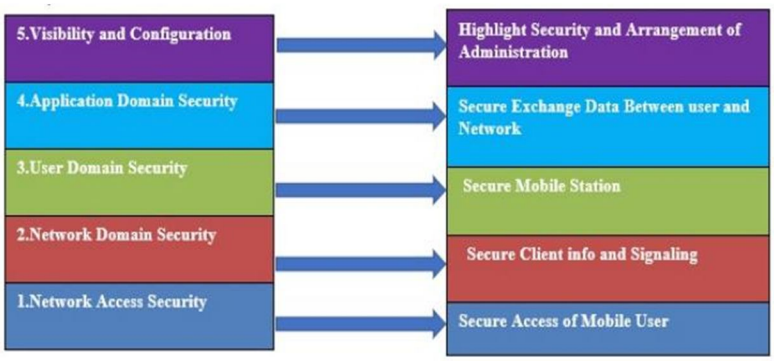


Figure 1. LTE security layers

III. VULNERABILITIES ON LTE AND LTE-A SECURITY

In light of (HE et al., 2018) review, they introduced a far reaching research concentrate on the LTE and LTEA network security assaults and they characterized the assaults as gatherings and they represented their consequences for LTE and LTE-An organizations. This part surveys the assaults and their dangers on LTE as introduced in Figure Based on (HE et al., 2018) review, they introduced a far reaching research concentrate on the LTE and LTE-A network security assaults and they characterized the assaults as gatherings and they represented their consequences for LTE and LTE-An organizations. This part surveys the assaults and their dangers on LTE as introduced in Figure 2.

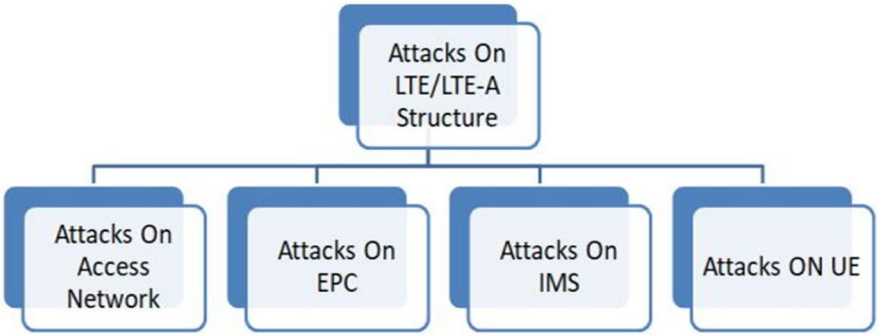


Figure 2. Attacks Classifications on LTE and LTE-A network.

A. Attacks on Access Network

(HE et al., 2018) examines a few issues that undermine 4G organization security like uncovering or finding the IMSI which alludes to International Mobile Subscriber Identity which is a vital part in LTE and LTE-An organizations. Finding the IMSI prompts spilling of the client's information which means breaking the security of the client. Besides, there is a danger in the capacity to follow the client's area by getting the area ID and PDA ID which has put the client at a high gamble. Also, there are more goes after in access organizations, for example, RF sticking, Spoofing and Sniffing, which are normal in actual layer assaults lead tasks/DDOS assaults (Mohapatra et al., 2015). The two assaults are not kidding and basic on LTE and LTE-An organizations since they make the CPU depleted and to not answer the administrations. DDOS assaulter can dominate a botnet which can get and utilize the casualty's data. There are likewise different interlopers on getting to networks for instance replay assaults and Eavesdropping assaults where as of recently LTE and LTE-A poor person has totally halted them.

B. Attacks on EPC (Evolved Packet Core)

There are many dangers that still danger LTE and LTE-A center organizations, for example, DOS and DDOS assaults which impact the HSS (Home Subscriber Server) that is the core of EPC networks since it contains the endorser's information, for example, IMSI and the assailant will make over-burdens on HSS and make it consume more assets and thus impact on the client gear conduct and SGW (Serving GateWay). There are likewise insiders goes after that influence the base station and close it. (HE et al., 2018)

C. Attacks on IMS

The SIP-related assault is the most genuine danger in IMS, for instance, SIP-flooding assaults. This assault can cause asset fatigue and result in DOS assaults and furthermore can send off additional assaults on IMS like VOLTE (Voice over LTE) and SMS. The assaults on VOLTE can taint the LTE organization and connection it back to the past circuit switch framework. Instances of VOLTE assaults, SIP flooding DOS assault, quiet call assaults, VOLTE spamming, mocking and phishing. Additionally, there are other not kidding assaults on SMS which is viewed as central in any portable assistance and it depends on the IMS framework. Figure 3 shows the design of the assaults on Another sort of assault is Abnormal charging in VOLTE. The assailant can get the information in for nothing through VOLTE administrations and this can prompt a DOS assault. Peng and others referenced three sorts of assaults of information charging on VOLTE. The first is free charging which can get to the information by utilizing IP caricaturing, the second is an extortion charging assault where assaults lay out a connection with a spamming server and send wrong data to the casualty so the charging will profoundly increase. The keep going assault on VOLTE is cheating, this assault can change the IP bundle time to live along these lines the parcels are dismissed when they are accounted for. There are more goes after on IMS like TCP/SYN flooding assaults and SQL infusion assaults. In view of (Mohapatra et al., 2015) various clients can connect with LTE network which empowers malevolent assaults, worm assaults, spam email, changing information and taking the quantity of charge cards in banking.

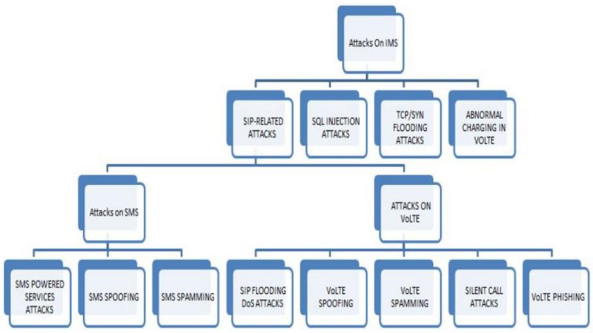


Figure 3. Structure of attacks on IMS.

D. Attacks on End User Equipment

This sort of assault contaminates the gadgets of the clients which frames a high effect of dangers on client's security, for example, botnet and malware. The previous can take any sort of information from the casualty, for example, SMS, email and a lot more while the last option can be utilized by aggressors to mishandle portable clients through sending off assaults to the organization, for example, DOS assault, SMS assault and unusual charging assault. As referenced by Ahlawat et al. (2018), there are different likely weaknesses in the LTE network which is partitioned into three angles; the first is the inside network remembered for the entrance and the center organizations; the second is the outside network which implies the approaching assaults from an outsider. The third viewpoint is the assaults coming from the client's gear. Moreover, the creator planned a structure that incorporates six classifications of LTE weakness as depicted in Figure 4. The creator additionally sorts the assaults in light of the LTE layers networks which comprise of five layers as referenced in the LTE security engineering segment (Ahlawat et al., 2018).

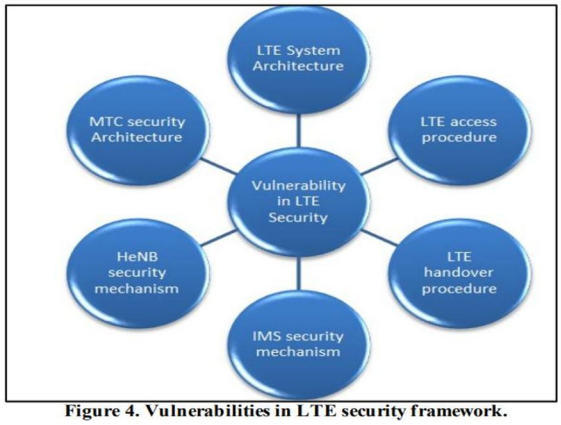


Figure 4. Vulnerabilities in LTE security framework.

IV. IMPROVEMENTS ON SECURITY ASPECT OF 4G/LTE NETWORK

This part showed the enhancements that have been finished with the security of the LTE and LTE-An organization according to alternate points of view and summed up them as per the year from 2014 as of not long ago in a rising request in the Table (1) beneath, subsequently anybody can take an outline on them and comprehend how the improvements on LTE security have been finished.

A. Alyaa Ghanim 2014

Distributed an examination on LTE cryptographic calculations relying upon different factors, for example, equipment execution, security and intricacy assaults (Sulaiman et al., 2014).

B. Soran Sabah Hussein 2014

Proposed a clever classification calculation by involving the replacement idea and dissemination wherein the necessary security level is achieved in only one round. Simultaneously, the intricacy is decreased impressively while the security is exceptionally expanded. (Hussein, 2014)

C. Madhusanka Liyanage 2015

Propose an application in light of SDN and NFV innovation to work on the security of the inheritance LTE instrument and defeat the LTE impediments and he referenced the upsides of the SDN in view of safety design (Liyanage et al., 2015)

D. Sumant Ku Mohapatra 2015

Planned a system comprising four layers to give an elevated degree of safety. The structure comprises of two sections the first is the fringe and the second is the center which coordinated to give predictable different correspondence organizations (Mohapatra et al., 2015)

E. Nicholas DeMarinis 2015

Provided a method to improve the security issue on the LTE network through recognizing the issues that exist in the prerequisite of the LTE security and afterward he planned a language to express a convention in the LTE network layer developing the compiler that interprets the convention and executing it.
At last, he proposed a few suggestions for future works (DeMarinis, 2015)

F. Brian Cusack 2016

Utilized an inventive recognition technique for the DDOS assault with detail and he talked about the advantages of utilizing his strategy for uncovering the sluggish DDOS assault. (Cusack et al., 2016)

G. Okoye Emmanuel Ekene 2016

Made or proposed an alteration in EPS-AKA which alluded to advanced parcel framework confirmation and key understanding in LTE network by utilizing PKI which is a reference to public key foundation and this change will safeguard IMSI which plays the primary part in LTE network security. (Ekene et al, 2016)

H. Yun Ye 2016

Examined and proposed strategies to working on the throughput of the LTE framework and furthermore outlined on LTE range sharing innovation in three kinds of spectrum(Ye et al., 2016)

I. Mohamed Amine Ferrag 2017

Did an extensive overview on four and five ages of portable organization particularly from the validation and security angles and he proposed open issues for future examination on confirmation and protection to guard 4G and 5G time from any intruders(Ferrag, 2017)

J. Eman Ashraf Mohammed 2017

Proposed another original calculation which depends on the RC6 calculation by consolidating of the two RC6 in one calculation to get 256 digit rather than 128 bit to support the speed and increment the security level contrasting and EEA2 which is the second arrangement of the LTE cryptographic calculation. (Mohammed, 2017)

K. Mourad Abdeljebbar and Rachid El Kouch 2018

Proposed an answer for improvingEP Authentication by joining the effortlessness of arrangements and the full shared verification which got every one of the correspondences substances.Then the proposed solution tested by the AVISPA model (Abdeljebbar & Kouch,2018)

L. Alyaa Ghanim Sulaiman 2018

Altered the AES cryptographic calculation which is the center of the EEA2 calculation of the LTE network security by HISEC calculation which is a lightweight square code calculation to expand the security and reduction the expense (Sulaiman and ALDabbagh, 2018)

M. Raja Ettiane 2018

Proposed a way to deal with distinguish DDOS assault motioning on LTE network with 91% of exactness and with quick time which is around just 380 seconds (Ettiane et al., 2018)

N. Carol Davids 2018

Did an exploration on the pattern of the continuous correspondence toward 5G organization and he referenced that the SDN and the virtualization are the vital pieces of fostering the 4G toward 5G organization additionally he urges the analysts to work successfully to defeat the backhauls that exist in the 4G organization (Davids, 2018)

O. Fuwen Liu 2018

Introduced a clever plan utilized for 5G to lessen the shortcomings and weakness in 4G/LTE network with next with no impact on AKA convention and character the board process(Liu et al.,2018).

P. Xu Zhang 2019

Introduced an original plan for further developing the crisis correspondence in LTE network including UAV, information an inquiry and video return devices(Zhang et al.,2019).

Q. Abubakar Muhammad Miyim 2019

Assessed the exhibition of LTE network utilizing OMNeT++ test system and saw that LTE network is give great of voice call(Miyim and Wakili,,2019

R. Chi-Yu Li 2020

Introduced another security configuration named as MECsec to diminish the idleness in the Knowledge Management International Conference (KMICe) 2021, 1 February 2021 http://www.kmice.cms.net.my/32 cell organization (Li et al., 2020)

S. Febby Ronaldo 2020

Proposed a plan for further developing security which is proficient in handling season of encoding and decoding information by utilizing three distinct calculations (Ronaldo et al.,2020)

V. DISCUSSIONS

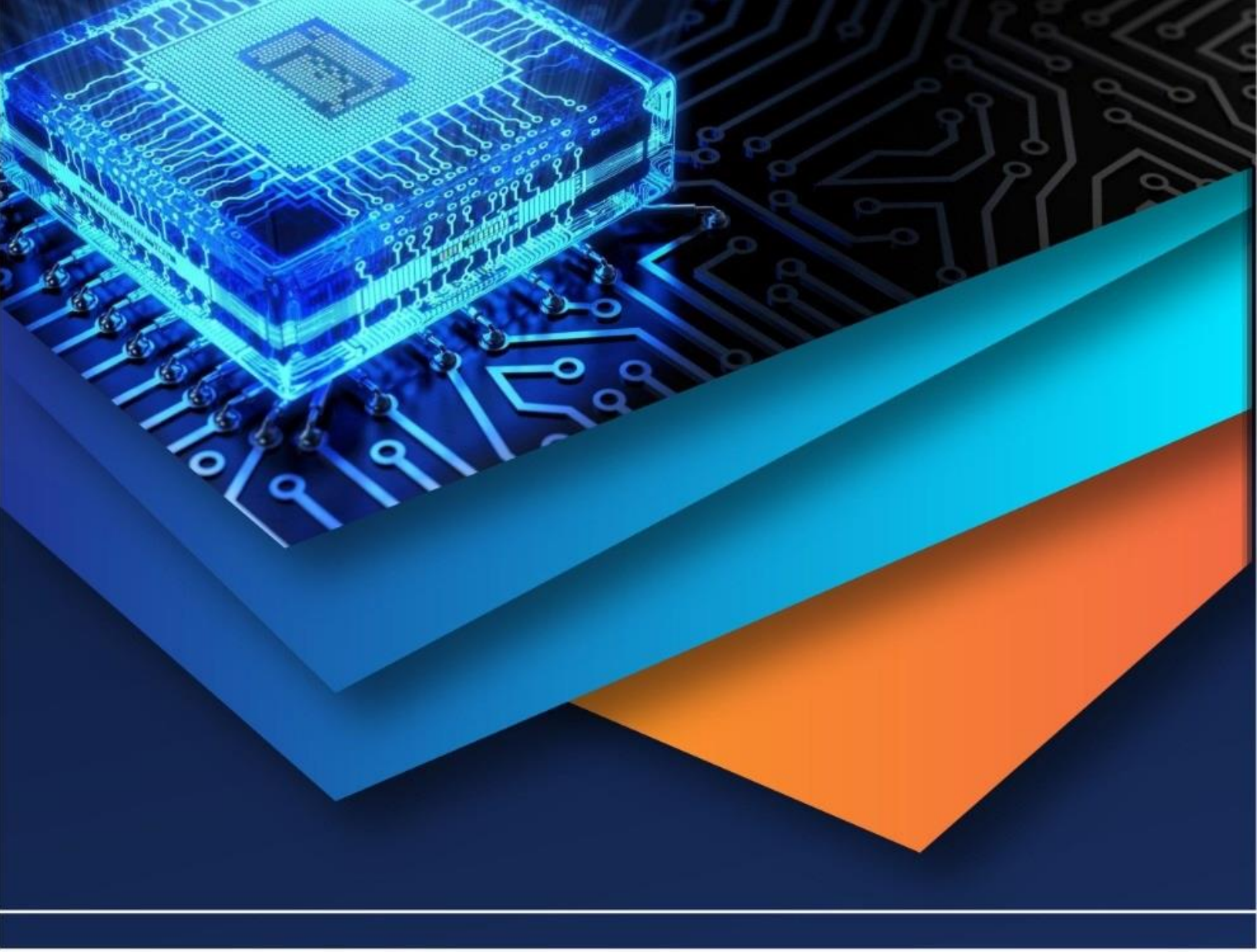
This paper talks about two inverse issues of the 4G/LTE network security which are the weaknesses and enhancements and shows the ongoing examinations that have been done on this organization according to alternate points of view. Thus, this will add adequate information for analysts who need to look and examine this field.

VI. CONCLUSION

In a nutshell, this article plans to accumulate a few issues in the weaknesses in LTE network security that as of late have been done to distinguish the holes or the difficulties which need to defeat to accomplish an elevated degree of safety and keep away from the aggressors from taking or keeping an eye on any private data or closing down the LTE/LTE-An organization. Besides, it endure the enhancements that have been done up to this point to help the fourth-age network's security.

REFERENCES

[1] Ahlawat, A., & Kumar, S. (2018). Investigating Various Possible Attacks and Vulnerabilties in LTE.
[2] Abdeljebbar, M., & El Kouch, R. (2018). Security Improvements of EPS-AKA Protocol. IJ Network Security, 20(4), 636-644.
[3] Cusack, B., Lutui, R., & Khaleghparast, R. (2016). Detecting Slow DDos Attacks on Mobile Devices.
[4] Davids, C., Gurbani, V. K., Ormazabal, G., Rollins, A., & Singh, K. (2018). Research topics related to real-time communications over 5G networks. ACM SIGCOMM Computer Communication Review, 46(3), 8.
[5] DeMarinis, N. A. (2015). On LTE Security: Closing the Gap Between Standards and Implementation.
[6] Ekene, O. E., Ruhl, R., & Zavarsky, P. (2016, June). Enhanced user security and privacy protection in 4g lte network. In Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual (Vol. 2, pp. 443-448). IEEE.
[7] Ettiane, R., Chaoub, A., & Elkouch, R. (2018, May). Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks. In Electrotechnical Conference (MELECON), 2018 19th IEEE Mediterranean (pp. 62-67). IEEE.
[8] Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., & Janicke, H. (2018). Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, 101, 55-82.
[9] He, L., Yan, Z., & Atiquzzaman, M. (2018). LTE/LTE-A Network Security Data Collection and Analysis for Security Measurement: A Survey. IEEE Access, 6, 4220-4242.
[10] Hussein, S. (2014). Lightweight security solutions for LTE/LTE-A Networks (Doctoral dissertation, Paris 11).
[11] Liyanage, M., Ahmad, I., Ylianttila, M., Gurtov, A., Abro, A. B., & de Oca, E. M. (2015, December). Leveraging LTE security with SDN and NFV. In Industrial and Information Systems (ICIIS), 2015 IEEE 10th International Conference on (pp. 220-225). IEEE.
[12] Li, C. Y., Lin, Y. D., Lai, Y. C., Chien, H. T., Huang, Y. S., Huang, P. H., & Liu, H. Y. (2020). Transparent AAA Security Design for Low-Latency MEC-Integrated Cellular Networks. IEEE Transactions on Vehicular Technology, 69(3), 3231-3243.
[13] Liu, F., Peng, J., & Zuo, M. (2018, August). Toward a secure access to 5G network. In 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE) (pp. 1121-1128). IEEE.
[14] Miyim, A. M., & Wakili, A. (2019, December). Performance Evaluation of LTE Networks. In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO) (pp. 1-6). IEEE.
[15] Mohammed, E. A., Areed, N. F., Takieldeen, A., & Abd-elazeem, M. (2017). Novel Cryptographic Algorithm for 4G/LTE-A. International Journal of Computer Applications, 163(1).
[16] Mohapatra, S. K., Swain, B., & Das, P. (2015). Comprehensive survey of possible security issues on 4G networks. International Journal of Network Security & Its Applications, 7(2), 61.
[17] Ronaldo, F., Pramadihanto, D., & Sudarsono, A. (2020, September). Secure Communication System of Drone Service using Hybrid Cryptography over 4G/LTE Network. In 2020 International Electronics Symposium (IES) (pp. 116-122). IEEE.
[18] Sulaiman, A. G., & AlDabbagh, S. S. M. (2018). Modified 128-EEA2 Algorithm by Using HISEC Lightweight Block Cipher Algorithm with Improving the Security and Cost Factors. Indonesian Journal of Electrical Engineering and Computer Science, 10(1), 337-342.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY