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

Alyaa Ghanim Suliaman, Zahraa Mazin Taha Alkattan
Software engineering Dept., Mosul University, Iraq {alyaa.ghanim@uomosul.edu.iq,zahraa.alkattan@uomosul.edu.iq}

ABSTRACT

Network security is considered a significant issue in our daily life due to its entering into many people's activities such as social activity, marketing and business. However, the need for a secure and powerful network has increased. The needs for a secure network have increased due to the increasing threats and hackers in our daily life. In fact, based on the current statistics, each second the number of subscribers is increasing by 10 times worldwide which refers to the fast growth of 4G /LTE networks. It is noticed that 80 percent of people globally have owned 4G mobile phones and the number is increasing during the recent several years. Furthermore, 4G/LTE is the foundation of the 5G network, so advanced security is needed. From this point, this paper presents a survey of the improvements that have been done recently on 4G/LTE security and reveals the weaknesses that still exist and that will allow researchers to focus and work on these weaknesses.

Keywords: Attacks, 4G/LTE, vulnerability and security.

I INTRODUCTION

The evolvements of fourth generation cellular network is up to date news nowadays. The trend toward developing and getting more reliable and authentic devices is increasing year by year. Hence, the researchers dedicate their time investigating and finding the solution for any backhaul or problem which still exists until now in the fourth generation of mobile communication. Based on (Ahlwat, 2018), the evolution from single authentication in the first generation to the mutual authentication in the 4G/LTE networks has made the network prone to new kinds of threats and vulnerabilities. The design of LTE is suitable for the demands of customer for getting fast access to data, less delay, high throughputs and high data rates. All these features motivate researchers to investigates more and works to improve and protect LTE security from any intruder. Therefore, this research surveys the recent improvements and developments on LTE security as well as figuring out the vulnerabilities that still exist in the LTE network and need to recover.

II LTE AND LTE-A SECURITY DESIGN

The design of LTE and LTE-A network consists of two main components, The first is Evolved Universal Terrestrial Radio Access network (E-UTRAN) and the second is Evolved Packet Core (EPC).Only a few surveys have been done to support LTE security and show the possible threats and recent improvements in LTE security. However, LTE security system architecture consists of five layers which are defined by the Third Generation Partnership Project (3GPP):

1. Network Access Security: Responsible for securing the access of the mobile users to the network and guaranteeing the radio access link is secured from any attack.
2. Network Domain Security: guarantees that portable backhaul hubs to safely trade signaling information and client information at the versatile backhaul systems and secures against assaults on wireline connection.
3. User Domain Security: Safe access to the mobile station.
4. Application domain security: This permit applications from the user and network considerations to securely interchanging data.
5. Visibility and Configuration of security: Permits clients to use data around empowered security highlights and arrangement of administrations. The layers are shown in Figure 1(Liyanage et al., 2015).

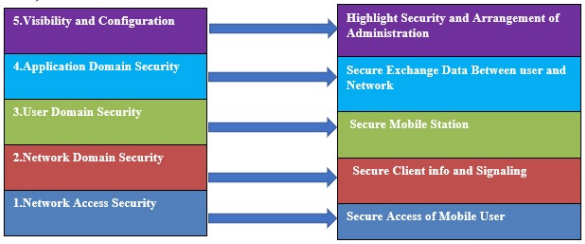

Figure 1. LTE security layers

III VULNERABILITIES ON LTE AND LTE-A SECURITY

Based on (HE et al., 2018) studies, they presented a comprehensive research study on the LTE and LTE-A network security attacks and they classified the attacks as groups and they illustrated their effects on LTE and LTE-A networks. This part reviews the attacks and their threats on LTE as presented in Figure 2.

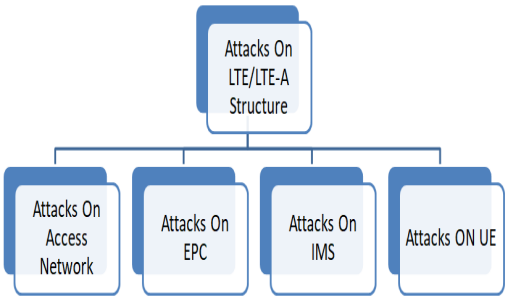

Figure 2. Attacks Classifications on LTE and LTE-A network.

A. Attacks on Access Network

(HE et al., 2018) discusses some issues that threaten 4G network security such as revealing or discovering the IMSI which is referred to International Mobile Subscriber Identity which is a very important part in LTE and LTE-A networks. Discovering the IMSI leads to leaking of the user's data which means breaking the privacy of the user. Furthermore, there is a threat in the ability to track user's location by getting the location ID and cell phone ID which has put the user at a very high risk. Moreover, there are more attacks in access networks such as RF jamming, Spoofing and Sniffing, which are common in physical layer attacks lead to DOS/DDOS attacks (Mohapatra et al., 2015). Both attacks are serious and critical on LTE and LTE-A networks because they make the CPU exhausted and to not respond to the services. DDOS assaulter can master a botnet which can get and use the victim's information. There are also other intruders on accessing networks for example replay attacks and Eavesdropping attacks where until now LTE and LTE-A have not been completely stopped them.

B. Attacks on EPC (Evolved Packet Core)

There are many risks that still threat LTE and LTE-A core networks such as DOS and DDOS attacks which influence the HSS (Home Subscriber Server) that is the heart of EPC networks because it contains the subscriber's data such as IMSI and the attacker will make overloads on HSS and cause it to consume more resources and consequently effect on the user equipment's behaviour and SGW (Serving GateWay). There is also insider attacks that affect the base station and shutdown it. (HE et al., 2018)

C. Attacks on IMS

The SIP-related attack is the most serious threat in IMS, for example, SIP-flooding attacks. This attack can make resource exhaustion and result in DOS attacks and also can launch further attacks on IMS like VOLTE (Voice over LTE) and SMS. The attacks on VOLTE can infect the LTE network and link it back to the previous circuit switch system. Examples of VOLTE attacks, SIP flooding DOS attack, silent call attacks, VOLTE spamming, spoofing and phishing. Also, there are other serious attacks on SMS which is considered fundamental in any mobile service and it is based on the IMS system. Figure 3 shows the structure of the attacks on Another kind of attack is Abnormal charging in VOLTE. The attacker can get to the data in free of charge through VOLTE services and this can lead to a DOS attack. Peng and others mentioned three kinds of attacks of data charging on VOLTE. The first is free charging which can get to the data by using IP spoofing, the second is a fraud charging attack where attacks establish a link with a spamming server and send wrong information to the victim so the charging will highly increase. The last attack on VOLTE is overcharging, this attack can change the IP packet time to live therefore the packets are rejected when they are accounted. There are more attacks on IMS such as TCP/SYN flooding attacks and SQL injection attacks. Based on (Mohapatra et al., 2015) many different users can interact with LTE network which enables malicious attacks, worm attacks, spam email, changing data and stealing the number of credit cards in banking.

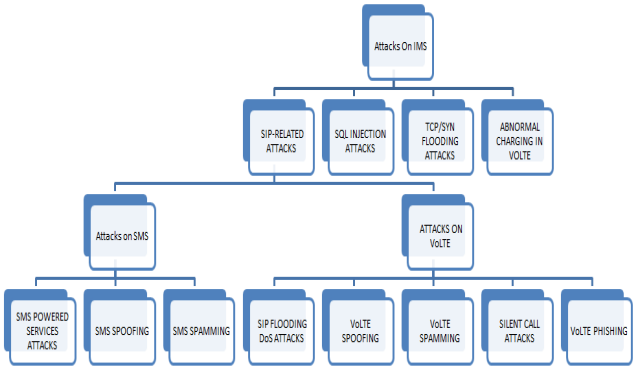

Figure 3. Structure of attacks on IMS.

D. Attacks on End User Equipment

This type of attack infects the devices of the users which forms a high impact of threats on user's privacy such as botnet and malware. The former has the ability to steal any kind of data from the victim such as SMS, email and many more while the latter can be used by attackers to abuse mobile user through launching attacks to the network such as DOS attack, SMS attack and abnormal charging attack. As mentioned by Ahlawat et al. (2018), there are various probable vulnerabilities in LTE network which is divided into three aspects; the first is the internal network included in the access and the core networks; the second is the external network which means the coming attacks from a third party. The third aspect is the attacks coming from the user's equipment. In addition, the author designed a framework that includes six categories of LTE vulnerability as described in Figure 4. The author also categorizes the attacks based on the LTE layers networks which consist of five layers as mentioned in the LTE security architecture section (Ahlawat et al., 2018).

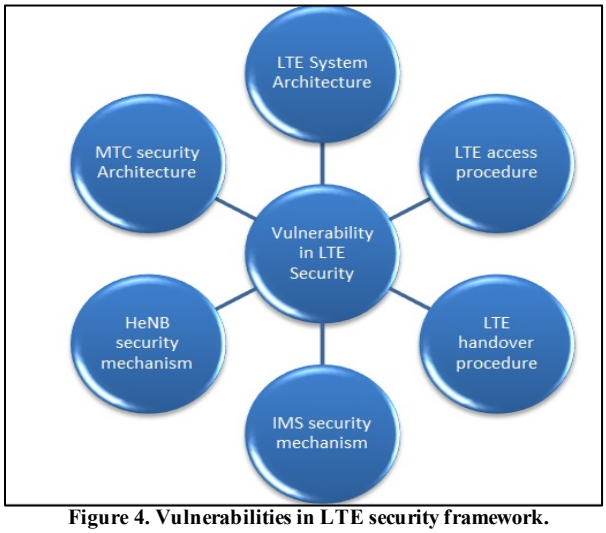

Figure 4. Vulnerabilities in LTE security framework.

IV IMPROVEMENTS ON SECURITY ASPECT OF 4G/LTE NETWORK

This section showed the improvements that have been done with the security of the LTE and LTE-A network from different perspectives and summarized them according to the year from 2014 until now in an ascending order in the Table (1) below, thus anyone can take an overview on them and understand how the developments on LTE security have been done.

Table 1. Survey on improvement on LTE/LTE-A network Security.

Author	Year	Contribution
Alyaa Ghanim	2014	Published a comparison on LTE cryptographic algorithms depending on various factors such as hardware performance, security and complexity attacks (Sulaiman et al., 2014).
Soran Sabah Hussein	2014	Proposed a novel confidentiality algorithm by using the substitution concept and diffusion in which the required security level is attained in only one round. At the same time, the complexity is reduced considerably while the security highly increased. (Hussein, 2014)
Madhusanka Liyanage	2015	Propose an application based on SDN and NFV technology to improve the security of the legacy LTE mechanism and overcome the LTE limitations and he mentioned the advantages of the SDN based on security architecture (Liyanage et al., 2015).
Sumant Ku Mohapatra	2015	Designed a framework consisting of four layers to provide a high level of security. The framework consists of two parts the first is the peripheral and the second is the core which organized to provide consistent different communication networks (Mohapatra et al., 2015)
Nicholas DeMarinis	2015	Supplied a technique to enhance the security issue on the LTE network through identifying the problems that exist in the requirement of the LTE security and then he designed a language to state a protocol in LTE network layer evolving the compiler that translate the protocol and implementing it. Finally, he suggested some recommendations for future works (DeMarinis, 2015)

Brian Cusack	2016	Used an innovative detection method of the DDOS attack with detail and he discussed the benefits of using his method of revealing the slow DDOS attack. (Cusack et al., 2016)
Okoye Emmanuel Ekene	2016	Made or proposed a modification in EPS-AKA which is referred to evolved packet system authentication and key agreement in LTE network by using PKI which is a reference to public key infrastructure and this change will protect IMSI which has the main role in LTE network security. (Ekene et al, 2016)
Yun Ye	2016	Discussed and proposed methodologies to improving the throughput of the LTE system and also overviewed on LTE spectrum sharing technology in three types of spectrum (Ye et al., 2016)
Mohamed Amine Ferrag	2017	Did a comprehensive survey on four and five generations of mobile network especially from the authentication and privacy aspects and he suggested open issues for future research on authentication and privacy to keep 4G and 5G era safe from any intruders (Ferrag, 2017)
Eman Ashraf Mohammed	2017	Proposed a new novel algorithm which is based on the RC6 algorithm by combining of the two RC6 in one algorithm to get 256 bit instead of 128 bit to boost the speed and increase the security level comparing with EEA2 which is the second set of the LTE cryptographic algorithm. (Mohammed, 2017)
Mourad Abdeljebbar and Rachid El Kouch	2018	Proposed a solution for improving EP Authentication by combining the simplicity of deployments and the full mutual authentication which secured all the communications entities. Then the proposed solution tested by the AVISPA model (Abdeljebbar & Kouch,2018)
Alyaa Ghanim Sulaiman	2018	Modified the AES cryptographic algorithm which is the core of the EEA2 algorithm of the LTE network security by HISEC algorithm which is a lightweight block cipher algorithm in order to increase the security and decrease the cost (Sulaiman & ALDabbagh, 2018)
Raja Ettiane	2018	Proposed an approach to detect DDOS attack signalling on LTE network with 91% of accuracy and with fast time which is around only 380 seconds (Ettiane et al., 2018)
Carol Davids	2018	Did a research on the trend of the real-time communication toward 5G network and he mentioned that the SDN and the virtualization are the key parts of developing the 4G toward 5G network also he encourages the researchers to work effectively to overcome the backhauls that exist in the 4G network (Davids, 2018)
Fuwen Liu	2018	Presented a novel scheme used for 5G to reduce the weaknesses and vulnerability in 4G/LTE network without any effect on AKA protocol and identity management process (Liu et al.,2018).
Xu Zhang	2019	Presented a novel design for improving the emergency communication in LTE network including UAV, data a question and video return devices (Zhang et al.,2019).
Abubakar Muhammad Miyim	2019	Evaluated the performance of LTE network using OMNeT++ simulator and noticed that LTE network is provide high quality of voice call (Miyim & Wakili,,2019)
Chi-Yu Li	2020	Presented a new security design named as MECsec to decrease the latency in the

		cellular network (Li et al., 2020)
Febby Ronaldo	2020	Suggested a scheme for improving security which is efficient in processing timeof encrypting and decrypting data by using three different algorithms (Ronaldo et al.,2020)

V DISCUSSIONS

This paper discusses two opposite issues of the 4G/LTE network security which are the vulnerabilities and improvements and shows the current studies that have been done on this network from different perspectives. So, this will add a sufficient knowledge for researchers who want to search and investigate on this field.

VI CONCLUSION

In a nutshell , this article intends to gather some issues in the vulnerabilities in LTE network security that recently have been done to identify the gaps or the challenges which need to overcome to achieve a high level of security and avoid the attackers from stealing or spying on any personal information or shutting down the LTE/LTE-A network. Furthermore, it survived the improvements that have been done until now to boost the fourth-generation networks security.

REFERENCES

Ahlawat, A., & Kumar, S. (2018). Investigating Various Possible Attacks and Vulnerabilties in LTE.

Abdeljebbar, M., & El Kouch, R. (2018). Security Improvements of EPS-AKA Protocol. *IJ Network Security*, *20*(4), 636-644.

Cusack, B., Lutui, R., & Khaleghparast, R. (2016). Detecting Slow DDos Attacks on Mobile Devices.

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.

DeMarinis, N. A. (2015). On LTE Security: Closing the Gap Between Standards and Implementation.

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.

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.

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.

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.

Hussein, S. (2014). *Lightweight security solutions for LTE/LTE-A Networks* (Doctoral dissertation, Paris 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.

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.

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.

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.

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).

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.

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.

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.

Sulaiman, A. G., & Al Shaikhli, I. F. (2014). Comparative study on 4G/LTE cryptographic algorithms based on different factors. International Journal of Computer Science and Telecommunications, 5(7), 7-10.

Ye, Y., Wu, D., Shu, Z., & Qian, Y. (2016). Overview of LTE spectrum sharing technologies. *database*, *54*(60), 76-88.

Zhang, X., Liu, D., Yuan, P., Wang, W., Cheng, X., Jia, W., & Qiu, Y. (2019, April). Architecture Design of Electric Power Emergency Communication Based on 4G LTE Network. In *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)* (pp. 600-603). IEEE.