5G Network Security: Unraveling Vulnerabilities and Innovating Defense Mechanisms

Mamoon M. Saeed[1], Elmustafa Sayed Ali[2(✉)], Othman O. Khalifa[3], and Rania A. Mokhtar[4]

[1] Department of Communications and Electronics Engineering, Faculty of Engineering, University of Modern Sciences (UMS), Sana'a, Yemen

[2] Department of Electrical and Electronics Engineering, Red Sea University (RSU), Port Sudan, Sudan

elmustafasayed@gmail.com

[3] Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia

[4] Department of Computer Engineering, College of Computers and Information Technology, Taif University, P.O. Box 11099, Taif 21944, Saudi Arabia

Abstract. Rapid developments in cellular communications are accompanied by rising privacy and security worries. Many people refrain from participating in activities like social networking, shopping, transactions, and conducting a lot of business because network security and user privacy are major concerns in our daily lives. However, there is now a greater need for a private, highly secure business. This was accompanied by an increase in the requirements for it due to the growing hazards and programmers in our daily activities. The Fifth Generations (5G) groups are rapidly developing, as evidenced by the fact that the number of supporters is increasing by several times per second around the world in light of the ongoing revelations. According to statistics, 80% of people worldwide claim to use 5G mobile phones, and the percentage has been steadily rising for a very long time. A high level of security is also necessary because the 5G network serves as the basis for the 5G network. From there, this article gives an overview of some of the different 5G network vulnerabilities that can occur. Additionally, certain recent advancements in 5G security have revealed several flaws that still exist, allowing experts to concentrate on and fix these flaws.

Keywords: security · 5g · vulnerabilities · evolved packet core · network access security

1 Introduction

Today's news focuses on advancements in the 5G wireless network. The development and acquisition of more dependable and realistic technologies are becoming increasingly popular. As a result, the specialists focus on looking into and solving any issue or backlog that existed as recently as the fourth generation of flexible correspondence.

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 383–392, 2025.
https://doi.org/10.1007/978-3-031-81570-6_25

The organization is more vulnerable to new threats and vulnerabilities as a result of the transition from the first single confirmation to the shared verification in the 5G/LTE Advanced (LTE-A) networks [1, 2]. Customers who demand quick information access, little lag time, high throughputs, and high information rates are catered to by the LTE-A network. These various factors urge researchers to carry out further studies and work to fortify and safeguard LTE-A security from gatecrashes. As a result, this inquiry evaluates the most recent developments in LTE-A security while also pointing out any problems the LTE-A organization may truly have and that it has to address [3].

As seen in the Figure, the Home Network, Serving Network, and Mobile Station (MS) were all involved in the 5G security process.

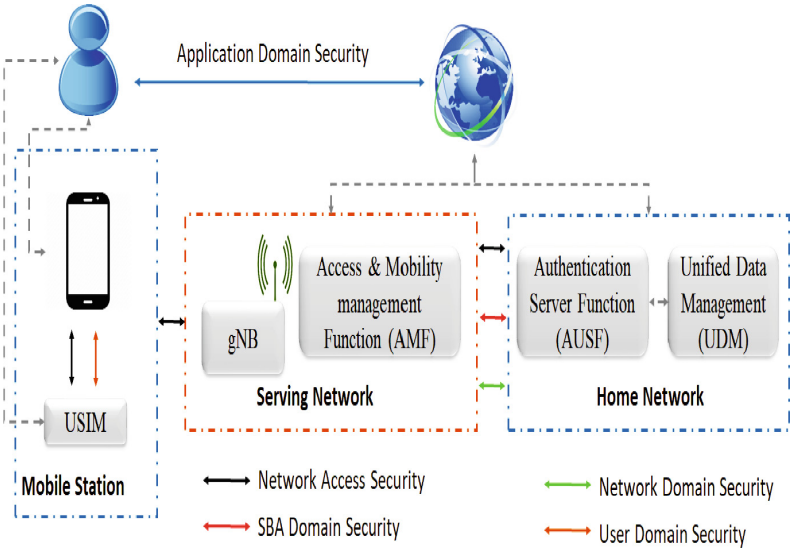

Fig. 1. 5G security architecture.

2 5G Security Design

The plan for 5G and Evolved Universal Terrestrial Radio Access Organization (E-UTRAN) and Evolved Packet Core are the two main components of an organization called Evolved Packet Core (EPC). Few overviews have been undertaken to help with LTE-A security, identify potential issues, and show progress being made in LTE-A security. Nevertheless, as illustrated in Fig. 2, the Third Generation Partnership Project (3GPP) has specified five tiers that comprise the LTE-A security framework.

- ***Network Access Security:*** protecting the radio access interface from threats and ensuring the organization's entrance for mobile clients.
- ***Security of Network Domain:*** protects against assaults on wireline connections and ensures that convenient backhaul center points safely exchange client and flagging data at flexible backhaul frameworks.

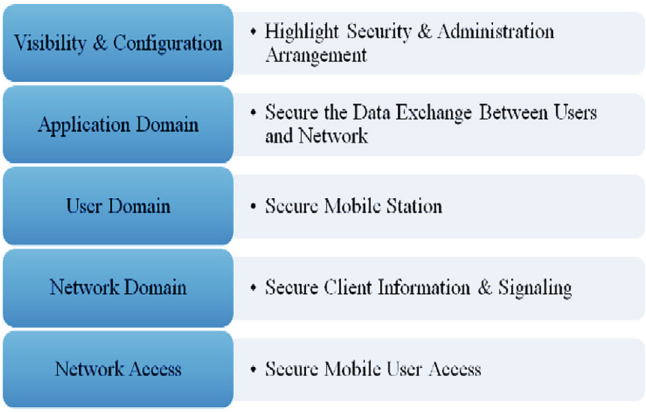

Fig. 2. 5G security Layers.

- ***Security of Client Domain:*** Access to the mobile station is secure.
- ***Security of Application:*** This permits programs from the customer and company to think about securely transferring data.
- ***Perceivability and Safety Configuration:*** gives users access to data on organizational strategy and activated security features. The layers [4] are displayed in Fig. 1.

3 Vulnerabilities on 5G Security

The information provided by the author in [5] led to a thorough research focus on 5G network security attacks. The attacks were categorized into groups, and they discussed how they had an impact on 5G companies. As indicated in Fig. 3, this section addresses the assaults and the dangers they represent to LTE-A. Based on the review by [5], they offered a comprehensive research focus on 5G network security attacks. They classified the attacks as groups and described how they affected 5G companies. This section examines the assaults and the risks they pose to 5G, as shown in Fig. 3.

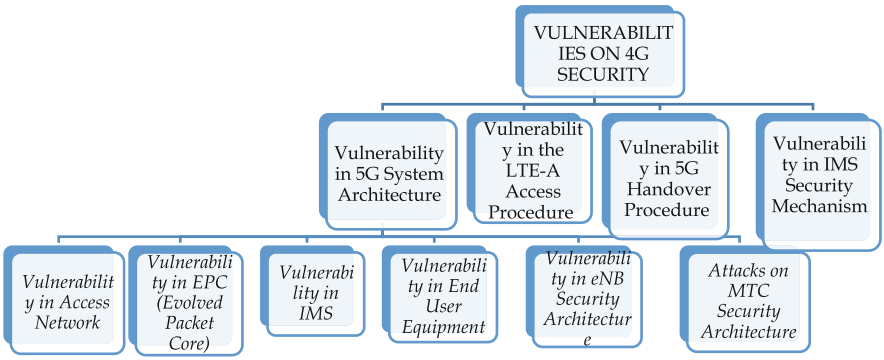

Fig. 3. Vulnerability in 5G System.

The following four parts of the 5G security framework may have vulnerabilities.

A. 5G System Architecture Vulnerability

Additional security problems are caused by the 3GPP LTE-A networks' flat IP-based architecture, which makes them vulnerable to attacks such as IP address spoofing, insertion, alteration, eavesdropping, DoS attacks, viruses, worms, spam emails, etc. In the flat design, an MME oversees several eNBs, giving malevolent attackers on the all-IP network a direct route to the base stations. Low-cost base stations called eNBs have made it simple for attackers to gain access so they can create their rogues. Due to various mobility situations, there are new risks when a UE shifts from one end to another [6, 7].

B. Vulnerability in Access Network

The authors in [5] look at a few problems that compromise the security of 5G organizations, such as discovering or locating the IMSI, or International Mobile Subscriber Identity, which is an essential component of 5G businesses. Finding the IMSI causes the client's information to be disclosed, which results in the client's security being violated.

The client is also at significant risk because it is possible to track the client's whereabouts by obtaining the area ID and PDA ID. Assaults like RF sticking, spoofing, and sniffing are also more common in access organizations and are widely used in real-layer attacks and DDOS attacks [8, 9]. The two attacks are crucial for 5G businesses because they drain the CPU and stop it from responding to service requests.

A botnet that can obtain and use the victim's data can be controlled by a DDOS attacker. There are other types of network intrusions as well, such as replay attacks and eavesdropping attacks, however, 5G has lately completely stopped them.

C. Vulnerability in EPC (Evolved Packet Core)

Regarding 5G, significant worries continue to exist. Because the HSS (Home Subscriber Server) is the hub of EPC networks and maintains the endorser's information, such as IMSI, attacks like DOS and DDOS will overwhelm the HSS (Home Subscriber Server), cause it to use up more resources, affect the behavior of client equipment, and have an impact on SGW (Serving Gateway). It has been documented that insiders can control base stations and shut them down [5].

D. Vulnerability in IMS

The biggest threat to IMS is an SIP-related attack, like an SIP flood attack. Resource depletion, DOS attacks, and the initiation of other IMS attacks like SMS and VOLTE-A could all result from this attack. VoLTE-A voice over LTE. Attacks against VOLTE-A could reflect poorly on the LTE-A organization and tie it to the outmoded circuit switch architecture. Attacks with VOLTE-A, SIP flooding DOS, quiet calls, VOLTE-A spamming, mocking, and phishing are a few examples. Additionally, significant attacks are launched against SMS, a component that is essential to any portable aid and is dependent on the IMS design. Attacks on aberrant charging in VOLTE-A are another type of attack, as seen in Fig. 3.

The attacker can get the data for free from VOLTE-A administrators, which could result in a DOS attack. Three potential methods of informational attacks against VOLTE-A were mentioned in some studies. The first is a free charging attack that uses IP caricature to access the information; the second is an extortion charging attack that connects to a spam server and provides false information to the victim to drastically increase the cost. The ongoing VOLTE-A attack is dishonest because it can give the IP

bundle time to live, releasing the packages after they have been accounted for. TCP/SYN flooding and SQL injection attacks are two other IMS attacks. Various clients can connect to an LTE-A network, allowing harmful attacks, worm attacks, spam emails, information modification, and the acceptance of a variety of credit cards for banking [10], according to [8].

E. Vulnerability in End User Equipment

This type of assault contaminates the client's devices with malware and botnets, dramatically raising the risk to the client's security. The former can be used to steal any kind of information from the victim, including SMS, email, and much more, whilst the latter can be used by attackers to exploit mobile users by starting attacks on the organization, such as DOS assaults, SMS attacks, and strange charge attacks. According to [1, 11], the LTE-A network, which is divided into three angles, has several potential faults.

The first is the internal network, which manages the entry and central businesses. The second is the outer network, which signals oncoming threats from the outside. Attacks coming from the client's equipment make up the third viewpoint. Furthermore, as depicted in Fig. 4, the architect created a building with six categories of LTE-A weaknesses. Additionally, by the LTE-A security engineering section, the designer categorizes the assaults into five different groups based on the LTE-A networks' five tiers [1].

F. eNB Security Architecture Vulnerability

Both the links between the UE and the eNB and the backhaul between the eNB and the EPC, make data and conversations susceptible to being intercepted and eavesdropped [12]. The current eNB security mechanism is unable to thwart various protocol attacks, including eavesdropping attacks, MitM attacks, masquerading attacks, and compromising subscriber access lists, as a result of a lack of strong mutual authentication between the UE and the eNB and the eNB's inadequacy as a trusted party.

G. Attacks on MTC Security Architecture

The MTC lacks security protocols for 3GPP networks, non-3GPP access, and communication between MTC applications and MTC devices. Additionally, there are no security mechanisms for communication between ePDGs and MTC devices. Since MTC devices usually need to have minimal capabilities in terms of both energy and computing resources, they are particularly vulnerable to a variety of attacks. These dangers include bodily harm, network intrusions, credential theft, and protocol attacks. When many MTC devices seek network access simultaneously, there may be signaling overhead between an HSS and the MME due to simultaneous authentication [13, 14].

H. Vulnerability in the LTE-A Access Procedure

The EPS-AKA program has no privacy protections. In other instances, the Globally Unique Temporary Identity system was unable to give the IMSI, therefore it had to be released (GUTI). It is unable to exchange messages with the active MME or retrieve the IMSI from it. Because the MME must send the UE's requests to the HSS/AuC before the UE has been validated by the MME, DoS attacks cannot be stopped. Only after getting a RES can the MME authenticate the UE.

The SN must go back to the HN to request a new set of When the UE stays in the SN for an extended amount of time and utilizes the entire set of its AVs for authentication, the SN must contact the HN to request a fresh set of authentication vectors. The result is

bandwidth usage and authentication signaling cost on the SN and HN. Numerous issues with the EAP-AKA protocol exist, such as user identity leakage, vulnerability to MitM attacks, sequence number (SQN) synchronization, and higher bandwidth usage [15–17]. The EAP-AKA or EAP-AKA' is recycled by the LTE-A system to offer secure access authentication.

I. 5G Handover Procedure Vulnerability

The current eNB can generate new keys for several target eNBs by chaining the current key with those parameters because the key chaining architecture is in use. An attacker will be able to obtain the keys for the following sessions after compromising the present eNB. By transmitting an LTE-Aring handover request message between eNBs or an S1 path switch acknowledgment message from an MME to a target eNB, a malicious eNB might prevent the NCC value from refreshing. The target eNB and the UE won't establish a security link, thus the UE must start a fresh handover operation [3, 15, 18–20].

J. Vulnerability in IMS Security Mechanism

Complexity of the system and energy use in UE The EPS AKA for LTE-A access authentication and the IMS AKA for IMS authentication are the two AKA protocols that an IMS UE is required to implement. IMS AKA is vulnerable to MitM attacks, has poor SQN synchronization, and uses more bandwidth. The registration request is received by the core network (I-CSCF/S-CSCF/HSS) from the P-CSCF/MME and is used to implement access authentication. However, by flooding the I-CSCF/S-CSCF/HSS with legitimate packets that contain inaccurate IMSI/IMPI, an attacker could conduct a DoS attack [21–24].

4 Improvements in Security Aspects of 5G Network

This section describes the improvements that have been made to 5G organization security from various studies and sum them up as current contributions in Table 1 to provide a summary and comprehend how the improvements on LTE-A security have been done.

The weaknesses and improvements of the 5G/LTE-A network security are discussed in this article, along with the ongoing audits that have been performed on this organization from various angles. As a result, this will provide analysts who must look into and analyze this sector with enough knowledge.

Numerous security improvements have been found and added to 5G networks after thorough investigation and analysis. Implementing improved encryption methods and protocols to safeguard data in transit is one notable advance. Stronger encryption measures made possible by these developments make it far more difficult for unauthorized parties to intercept and decipher sensitive data.

The use of improved authentication and access control systems is a crucial component of the security upgrades in 5G networks. This minimizes the danger of unauthorized access and potential cyberattacks by ensuring that only authorized devices and users may connect to and access the network. Additionally, advances in network slicing have made it possible for various network segments to be isolated inside the 5G infrastructure, guaranteeing that any compromise in one segment would not affect the security or functionality of other parts. This isolation improves the network's overall security posture and lessens the effects of any potential intrusions.

Table 1. Related Works for Improvements on Security Aspect of 5G Network

Dataset	Best Accuracy Achieved & Author	Category	Number of actions (classes)
KTH	97.6% [Ziaeefard et al.']	General purpose Action recognition	6
Weizmann	100% [yangwang et al. 09; Lin et al. 09; Zeng and Ji et al.]	General purpose Action recognition	10
IXMAS	89.4% [Xinxiao Wu et al.']	Motion Acquisition	13
UCF Sports	93.5% [Simon Ones et al.']	Sports action	150
HAHA	56.8% [Andrew Gilbert et al.']	Movies	12
i3DPost Multi-View	80% [Michael B. Holte et al.']	Motion Acquisition	12
HMDB-51 (II)	Oh et al.	Movies	51
UCF-101 (IV)	Soomro et al.	Sports	101
Sports-1M (IV)	Karpathy et al.	Sports	487
ActivityNet (II)	Heilbron et al.	Human activities	203
NTU RGBD (II)	Shahroudy et al.	Human activities	60

The overall effects of these security upgrades have been encouraging. On 5G networks, researchers have noticed a sharp decline in security incidents and successful cyberattacks. Various known vulnerabilities and threats have been successfully mitigated by the strengthened access control, authentication, and encryption systems, creating a more secure environment for data transmission. However, it's crucial to remember that ongoing research and awareness are needed to keep ahead of potential security issues due to the permanence of cyber threats and the growth of technology. To maintain the security of 5G networks and successfully counter new threats, industry players, researchers, and regulatory agencies must continue to work together.

5 Conclusions

To identify the gaps or difficulties that must be overcome to achieve a higher level of security and prevent attackers from stealing or monitoring any private data or shutting down the 5G organization, this article aims to compile several issues relating to recent LTE-A network security flaws. It also maintains the level of development necessary to enable the security of the 5G network.

References

1. Ahlawat, A., Kumar, S.: Investigating various possible attacks and vulnerabilities in LTE-A (2018)
2. Saeed, M.M., et al.: Survey of privacy of user identity in 5G: challenges and proposed solutions. Saba J. Inf. Technol. Netw. (SJITN) **7**(1) 2019
3. Saeed, M.M., Saeed, R.A., Saeid, E.: Preserving privacy of paging procedure in 5thG using identity-division multiplexing. In: 2019 First International Conference of Intelligent Computing and Engineering (ICOICE). IEEE (2019)
4. Mukhtar, A.M., Saeed, R.A., Mokhtar, R.A., Ali, E.S., Alhumyani, H.: Performance evaluation of downlink coordinated multipoint joint transmission under heavy IoT traffic load. Wirel. Commun. Mob. Comput. **2022**, Article no. 6837780 (2022). https://doi.org/10.1155/2022/6837780
5. He, L., Yan, Z., Atiquzzaman, M.: LTE-A/LTE-A-A network security data collection, and analysis for security measurement: a survey. IEEE Access **6**, 4220–4242 (2018)
6. Saeed, M.M., et al.: A comprehensive review on the users' identity privacy for 5G networks. IET Commun. **16**(5), 384–399 (2022)
7. Macaulay, T.: The 7 deadly threats to 5G: 5G LTE-A security roadmap and reference design, vol. 25, p. 2017 (2013)
8. Pathak, P.H., et al.: Visible light communication, networking, and sensing: a survey, potential and challenges. IEEE Commun. Surv. Tutor. **17**(4), 2047–2077 (2015)
9. Saeed, M.M., et al., A novel variable pseudonym scheme for preserving privacy user location in 5G networks. Secur. Commun. Netw. 2022, 7487600 (2022)
10. DeMarinis, N.: On LTE-A Security: Closing the Gap Between Standards and Implementation. Worcester Polytechnic Institute (2015)
11. Saeed, M., et al., Preserving privacy of user identity based on pseudonym variable in 5G. Comput. Mater. Contin. **70**(3), 5551–5568 (2022)
12. Saeed, M.M., Saeed, R.A., Saeid, E.: Identity division multiplexing based location preserve in 5G. In: 2021 International Conference of Technology, Science and Administration (ICTSA). IEEE (2021)
13. Yan, X., Ma, M.: A privacy-preserving handover authentication protocol for a group of MTC devices in 5G networks. Comput. Secur. **116**, 102601 (2022)
14. Gupta, S., Parne, B.L., Chaudhari, N.S.: SRGH: a secure and robust group-based handover AKA protocol for MTC in LTE-A networks. Int. J. Commun. Syst. **32**(8), e3934 (2019)
15. Shaik, A., et al., Practical attacks against privacy and availability in 5G/LTE-A mobile communication systems (2015)
16. Elfatih, N.M., et al.: Internet of vehicle's resource management in 5G networks using AI technologies: current status and trends. IET Commun. **16**, 400–420 (2022). https://doi.org/10.1049/cmu2.12315
17. Wu, S., et al.: Identifying security and privacy vulnerabilities in 5G LTE-A and IoT communications networks. In: 2021 IEEE 7th World Forum on Internet of Things (WF-IoT). IEEE (2021)
18. Masud, M.: Survey of security features in LTE-A handover technology. System **1**(2) (2015)
19. Bitsikas, E., Pöpper, C.: Don't hand it over vulnerabilities in the handover procedure of cellular telecommunications. In: Annual Computer Security Applications Conference (2021)
20. Bikos, A.N., Sklavos, N.: LTE-A/SAE security issues on 5G wireless networks. IEEE Secur. Priv. **11**(2), 55–62 (2012)
21. Wang, D., Liu, C.: Model-based vulnerability analysis of IMS network. J. Netw. **4**(4), 254–262 (2009)

22. Saeed, M.M., et al.: A comprehensive review on the users' identity privacy for 5G networks. IET Commun. **16,** 384–399 (2022). https://doi.org/10.1049/cmu2.12327
23. Tu, G.-H., et al.: New security threats caused by IMS-based SMS service in 5G LTE-A networks. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (2016)
24. Lu, Y.-H., et al.: Ghost calls from operational 5G call systems: IMS vulnerability, call DoS attack, and countermeasure. In: Proceedings of the 26th Annual International Conference on Mobile Computing and Networking (2020)
25. Suliaman, A.G., Alkattan, Z.M.T.: Survey on vulnerability of 5G/LTE-A network security and improvements (2021)
26. Li, C.-Y., et al.: Transparent AAA security design for low-latency MEC-integrated cellular networks. IEEE Trans. Veh. Technol. **69**(3), 3231–3243 (2020)
27. Parameshachari, B., Panduranga, H., liberata Ullo, S.: Analysis and computation of encryption techniques to enhance the security of medical images. In: IOP Conference Series: Materials Science and Engineering. IOP Publishing (2020)
28. Miyim, A.M., Wakili, A.: Performance evaluation of LTE-A networks. In: 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). IEEE (2019)
29. Yu, W., et al.: Survey of public safety communications: user-side and network-side solutions and future directions. IEEE Access **6**, 70397–70425 (2018)
30. Muthana, A., et al.: Enhancing privacy of paging procedure in LTE-A. Int. J. Eng. Sci. Invent. **7**(2), 42–50 (2018)
31. Ferrag, M.A., et al., Security for 5G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. J. Netw. Comput. Appl. **101**, 55–82 (2018)
32. Liu, F., Peng, J., Zuo, M.: 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). IEEE (2018)
33. Saeed, R.A., Saeed, M.M., Mokhtar, R.A., Alhumyani, H., Abdel-Khalek, S.: Pseudonym mutable based privacy for 5G user identity. J. Comput. Syst. Sci. Eng. **29**(1), 1–14 (2021). https://doi.org/10.32604/csse.2021.015593Muthana
34. Jover, R.P., Lackey, J., Raghavan, A.: Enhancing the security of LTE-A networks against jamming attacks. EURASIP J. Inf. Secur. **2014**(1), 1–14 (2014)
35. Hussein, S.: Lightweight security solutions for LTE-A/LTE-A networks, Paris 11 (2014)
36. Sulaiman, A.G., AlDabbagh, S.: Modified 128-EEA2 algorithm by using HISEC lightweight block cipher algorithm with improving the security and cost factors. Indones. J. Electr. Eng. Comput. Sci. **10**(1), 337–342 (2018)
37. Premchander, T.: Survey on vulnerability of 5G/LTE-A network security and improvements
38. Liyanage, M., et al.: Leveraging LTE-A security with SDN and NFV. In: 2015 IEEE 10th International Conference on Industrial and Information Systems (ICIIS). IEEE (2015)
39. Mohapatra, S.K., et al.: Comprehensive survey of possible security issues on 5G networks. Int. J. Netw. Secur. Appl. **7**(2), 61 (2015)
40. Cheema, A., et al.: Prevention techniques against distributed denial of service attacks in heterogeneous networks: a systematic review. Secur. Commun. Netw. **2022**, 8379532 (2022)
41. Ekene, O.E., Ruhl, R., Zavarsky, P.: Enhanced user security and privacy protection in 5G LTE-A network. In: 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC). IEEE (2016)

42. Saeed, M.M., Saeed, R.A., Azim, M.A., Ali, E.S. , Mokhtar, R.A., Khalifa, O.: Green machine learning approach for QoS improvement in cellular communications. In: 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), pp. 523–528 (2022). https://doi.org/10.1109/MI-STA54861.2022.9837585
43. Davids, C., et al.: Research topics related to real-time communications over 5G networks. ACM SIGCOMM Comput. Commun. Rev. **46**(3), 1–6 (2018)
44. Elmustafa, S.A., et al.: Machine learning technologies for secure vehicular communication in internet of vehicles: recent advances and applications. Secur. Commun. Netw. **2021**, Article no. 8868355 (2021). https://doi.org/10.1155/2021/8868355
45. Alsaqour, R., Ali, E.S., Mokhtar, R.A., Saeed, R.A., Alhumyani, H., Abdelhaq, M.: Efficient energy mechanism in heterogeneous WSNs for underground mining monitoring applications. IEEE Access **10**, 72907–72924 (2022). https://doi.org/10.1109/ACCESS.2022.3188654