International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-3, May 2021
https://doi.org/10.55524/ijircst.2021.9.3.34
Article ID Article ID 219334, Pages 173-178
www.ijircst.org

A Review Study on 4G Security

Ms. Sania[1], Mr. Pankaj Saraswat[2], Ms. Swati[3]

[1]Assistant Professor, Department of Computer Application, Tecnia Institute of Advanced Studies, Delhi, India
[2,3]Assistant Professor, OEIT, Sanskriti University, Mathura, Uttar Pradesh, India

Correspondence should be addressed to Ms. Sania; ssaniasachdeva@gmail.com

ABSTRACT- The introduction of the Long Term Evolution (LTE) technology in recent technologies has revolutionized Fourth Generation, 4G Network communication, allowing users to receive high-speed data up to 100 MHz. The problem of cyber-security has become a menace to consumers all around the globe. This article will go through the LTE security concept. The next generations of wireless networks, known as 4G, will completely replace 3rd generation networks. It will provide faster speeds and multimedia services that are entirely IP-based. 4G refers to an integrated, worldwide network that will give customers with phone, data, and streaming multimedia services "Anytime, Anywhere." The smooth handoff, mobility management, security, and service across multiple integrated networks are all essential and demanding issues in 4G. Data security, hardware security, and user privacy and integrity are the most important security concerns for any wireless mobile device. Security flaws may be created by attackers or induced by incorrect device or network parameter settings. The paper explains the concept of security and why it is important to pay attention to it. This paper examines what 4G network technology is and some of the proposed solutions in order to fully understand the benefits and problems of successfully deploying 4G. The future aspects are this Network access security, which allows users to access the service in a safe and secure manner.

KEYWORDS- Data Security, Internet, Long Term Evolution, Networks, Security, Wireless Network.

I. INTRODUCTION

The 4G generation is the successor to the 2G as well as 3G standards families. Mobiles web access, gaming facilities, high-definition mobile TV, IP telephony as well as video are all available on mobile devices. Conferencing and 3D television are the two most popular options apps that make advantage of 4G cellular technology networks. Highly heterogeneous and changing throughout time the underlying protocol's quality of service the emergence of the layers is necessary. 3G and 4G wireless system applications 4G-enabled gadgets use their cellular connection to connect to the Internet. Instead of receiving a signal from an ISP, as it would at home or at work, the device receives data from a cellular carrier through a mobile phone connection. Users may connect to the Internet through 4G from everywhere there is a signal. Data sent via 4G is safer than data sent over public Wi-Fi since it is encrypted. MNOs may be lulled into a false feeling of security by the security design of 4G LTE, which assumes that the technologies inherently handles safety in LTE operations. There are known safety flaws in 4G LTE. Aside from fundamental LTE flaws, Four G LTE has long standing internets protocol (IP) founded security flaws.

The greatest need for internet connectivity wherever, whether at home or at work, as well as when traveling by vehicle, rail, or airline, Internet connectivity is available everywhere, at any time. Furthermore, there is a need for improved voice quality and speed. A network provider's success is determined by cheap costs and a wide range of services. The third Group Partnership Project (3GPP) is a global standards association that develops and standardizes mobile phone technology for the third generation. LTE is a big step forward in cellular technology[1].

The mobile network technology tree is a 3GPP initiative that is primarily designed for 3GPP cellular system families. It with an enhanced new radio interface, it is frequently referred to as E-UTRA & E-UTRAN network. Long into the next decade, LTE is expected to address carrier demands for higher speed data as well as media transfers, as well as high-capacity voice support. LTE is in a good position to address the needs of next-generation mobile networks. Operators will be able to offer excellent, mass-market mobile internet services by combining high bit rates and scheme throughput in both the downlink and uplink with low latency. All LTE network installations must fulfill the following minimum requirements: increased speed, multiple antennas, IP-based network with a new air interface: Duplexing, timing, carrier spacing, and coding are all part of OFDMA. LTE is constantly changing, and 3GPP publishes new versions on a regular basis[2], [3].

The key distinction is that, unlike WiMAX, which necessitates the construction of a new network, LTE is based on an extension of the existing UMTS infrastructure, which is currently in use by over 80% of mobile customers worldwide. This suggests that, despite mobile technology's fast growth, the LTE standards may lags beyond Mobiles WiMAX, while having a considerable incumbent advantage. The purpose of this article is to explore cyber-security challenges and to suggest that IPsec be utilized as one of the security measures[4].

A. Evolution of wireless technologies

After the launch of the 1st generation telephone networks in the early 1980s, the mobile wireless communications system has gone through numerous phases of development in the last several decades. Because there was such a high demand for new connections throughout the globe, mobile communication standards progressed quickly to accommodate more users. Let's have a looks at the various phases of wireless communication technology advancement[5], [6].

1) 1G

1G refers to the initial generation of mobile networks, which were created to offer clients with basic voice calling capabilities. 1G networks were first established in the 1980s in various regions of the globe using a variety of analogue cellular technology. These are analog communications technologies that were launched in the 1980s and lasted until 2G digital telecommunications supplanted them.

2) 2G

The second generation of mobile networks, which replaced the first generation, is referred to as 2G. These networks allowed users to have very secure phone calls, send SMS messages, and access limited mobile data capabilities. In the 1990s, several digital technologies were used to construct 2G networks in various parts of the world.

3) 2.5G

The second generation saw GSM (Global Systems for Mobile Communications) technologies become a standard in the early 1990s. For the first time, it allowed users to wander as well as transfer digital speech and data across the network. To improve the integrity and privacy of phone calls in 2G, signaling, data secrecy, as well as gsm network identification were all used.

4) 3G

Third-generation mobile communication, which initially became available in 2001, was meant to provide more voice and data capacity, as well as a larger variety of applications and improved data transfer at a cheaper cost. This generation was the first to provide both high-speed wide-band and fixed wireless internet connections, allowing users to make video calls, chat, and do other things. Network Access, Domains Security, as well as Application Security were among the new security features added in the third generation.

5) 4G

The 4th generations, which started in the years 2010, is a networks architecture that is entirely IP-based. Its goal is to provide higher quality, high-speed, as well as high-capacity phone and data services as well as internet over IP to customers while improving security and cutting costs. The fundamental benefits of an IP founded networks is that it can flawlessly migrate from previous generation infrastructure to voice and data technologies such as GSM, UMTS, and CDMA2000.

B. Privacy and Security

To guarantee that data transmissions are as safe as possible, security mechanisms must be introduced as part of the implementation of 4G networks. According to "the 4G center," "the 4G center" addresses "strength, safety, and QoS by reusing present approaches while still bothering to work on some mobility and surrender difficulties." As a consequence, the corporation will need to build a series of technologies that will support the bulk of 4G security processes as a way to protect data transferred over the networks against hackers as well as other security breaches. One of the most important goals of 4G networks is to deliver a consistent service throughout a vast geographic region. Smaller local area networks, on the other hand, will need their own operational systems. The fact that these wire-less networks transmit a variety of data further complicates the safety as well as confidentiality issue. Furthermore, whenever new devices and services are introduced to 4G networks for the first time. There are two options for dealing with these privacy and security problems.

1) Service Excellence

In terms of network dominance, numerous telecommunications firms believe that connectivity will improve and that the quality of information sent across the network will improve. The business guarantees that "The inventor's job Mobile phone did for influence, and 4G network technology will do the same for broadband. With when likened to today's mobiles broadband networks, the simultaneous display and advanced data rates are nearly ten times higher. Customers may be tracked at all times, even while they're on the road" [7]. As a result, providers must develop a cost-effective plan for extending their services to the 4G networks that will expand quality, offer proper security, and guarantee that all customers have a variety of alternatives for loading videos, music, as well as photo without needing to pay for delays. The integration of non-IP as well as IP-based devices is the major problem that 4G networks confront. Since non-IP address-based gadgets are often utilized for applications like VoIP, it is well-known. Devices that rely on IP addresses, on the other hand, are outmoded in terms of information propagation. Four G networks will support together types of devices. As a result, merging the ways for offering services to both non-IP as well as IP founded devices is a huge difficulty. A variety of challenges must be addressed by 4G networks.

2) IP Devices Integration

Non-IP as well as IP devices are combined in 4G technologies to give better services with larger data rates as well as bandwidths. This makes it possible for consumers to connect too many mobile wireless networks at the same time. Multimode software is the best explanation for this scenario. This is software that lets a user device to adapt to a range of wireless interface networks in order to give consistent internet connection at a high data rate. This is entirely based on packets.

3) Affordability and User Account Management

Maintaining customer accounts has become more difficult with 4G networks. The billing system cannot be worked out and handled because to the variety of 4G networks as well as the frequent involvement of various suppliers. There are a lot of aspects to consider in terms of Four G Networks pricing as well as affordability, including risk and time, in order for these networks to be viable once they are trolled out to the over-all population. In general, Four G networks are intended to provide an environments that allows higher speed data broadcasting as well as higher-than-before income margins for businesses who take use of these capabilities.

C. Challenges and Requirements for Security

The primary issue of every wireless mobile device is data, hardware, user identification, and privacy security. Attackers may originate security holes, or they can be caused by wrong network or user mobile parameter settings. For example, if a user's mobile settings are left open, any attacker may access the data; in another instance, even if the device has robust security protections, signaling at12tack might lead to resource abuse. Even if resources such as channel, bandwidth, and energy are available, the impacted mobile user will be refused access in certain instances. As a result, security mechanisms that can balance resource availability while attaining high QoS must be included in 4G systems. There are two types of security requirements for 4G heterogeneous networks: first, mobile communication devices, and secondly, operator networks. Protecting the integrity, privacy, as well as secrecy of the device, limiting data access, and preventing the theft of mobile equipment are all requirements for mobile equipment.

Prevailing research on the safety of four G heterogeneous networks has primarily concentrated on network-to-operator interfaces security challenges such as identification and authorization. Concerns about mobile computing security are now causing a number of issues. The capacity to move between networks and providers, resulting in vertical as well as horizontal handoffs, has considerably to the difficulty of mobile securities. As a consequence, security solutions must be built to be network, service provider, as well as end-user device agnostic. Data should be protected, but so should an institution that is 4G, which should secure both entities and infrastructure.

D. Threats and Attacks on 4g Security

In 4G networks, different wireless technology as well as service providers use an IP-based core network to provide continuous services to their clients with nearly the same quality of service (QoS). Four G heterogeneous networks understand new security vulnerabilities and attract attacks from the internet as a result of its open design and IP-based environment. A 4G network design may be vulnerable to a variety of attacks. IP address spoofing, User ID theft, Theft of Service (ToS), Denial of Service (DoS), and intrusion assaults are among the dangers. The network infrastructure was under the jurisdiction of the service providers, and access to other network devices was restricted. In 4G, there was a brand-new danger that had not been witnessed in 3G. When the end user device is removed from the internet owing to a lack of battery capacity, another risk with mobile communications privacy arises. When the device is turned on, it goes from being disconnected to being connected, enabling the attacker to pose as a mobile device or a mobile support station. Denial-of-service attacks, infections, worms, and other malware may also be spread through new end-user devices[9]. According to X.805, security concerns include information destruction, corruption, and alteration, theft, removal, or loss of information, disclosure of information, and service disruption[9].

E. Issues with 4g Security

The key security issues of any wireless mobile device are data security, hardware security, and user privacy and integrity. Attackers may originate security holes, or they can be caused by wrong device or network factor settings. For example, a user's mobiles settings are often left open, allowing any attacker access to the data, while in another case, despite the device's robust security protections, a continual signaling assault might lead to resource exploitation. Even if resources like as energy, channel, and bandwidth are available, the mobile user will be refused access in certain instances. As a consequence, 4G requires security measures that guarantee constant QoS while balancing resource availability. The security issues with a 4G network include:

- Application Security: The hardware, software, data, and operating system are all secure (OS). Integrity, Confidentiality, Verification, as well as Authorizations are the four pillars of network access security (CIAA).
- User security includes the identification, confidentiality, and authorisation of the user.
- Quality of Service (QoS) maintenance: protection against Denial of Services attacks in order to maintain a continuous QoS.

There are two types of security requirements for 4G heterogeneous networks: first, mobile communication devices, plus second, operator networks. Protecting the integrity, privacy, and confidentiality of the device, regulating data access, as well as keeping the mobile equipment from being attacked, as well as the information from being ill-treated or used as an outbreak weapon, are all requirements for mobile equipment. Authentication and authorization at the network-to-operator interface have been the subject of previous research on the safety of Four G hetero generous networks. On the other hand, protecting a mobile device against attacks as well as using it as an attack tool tackles significant securities issues in a heterogeneous networks.

Safeguarding mobile cranes, equipment integrity, and software integrity are all important aspects of mobile security. They don't prohibit mobile data access, and mobile devices may be used as a weapon. Mobile computing security problems are providing a growing number of challenges. The capacity to move between networks and providers, resulting in vertical as well as horizontal handoffs, has contributed to the complexity of mobile security. We may examine security risks related to the internet and IP security vulnerabilities since 4G networks are totally IP-based. New dangers include IP address spoofing, user Account theft, Denial of Services, Theft of Services, as well as penetration attacks. As a consequence, security solutions must be built to be network, internet provider, as well as end-user device agnostic. Not only should data be safeguarded, but a 4G organization should also secure its entities and infrastructure. Networks as well as service suppliers must ensure that their substructures as well as services are safe and that end users have secure access to and services.

1) *Issues with the physical layer*

At the physical layer, both WIMAX and LTE are vulnerable to two input flaws. A communication system may cease working owing to a high signal-to-noise ratio if man-made intervention is purposely inserted on an average. There are dual sorts of tampering that may be done: (i) noise as well as (ii) multicarrier. Noise interference is a technique that may be used. Gaussian white noise (WGN). The attacker detects carriers utilized by the victim in the event of multi-carrier interference. Organize the carriers and place a very narrowband signal on top of them. Interference assaults are simple to carry out. Because the tools and information necessary to counteract such assaults are readily accessible. Interference, according to our findings, is a problem.

Radio spectrum monitoring equipment makes it easy to spot. The interfering signal was located using radio-direction-finding equipment. It is possible to track down the source. In calculations, increasing the source signal's strength and using spreading methods may help. Increase its resistance to tampering. While the risk of interference is high, it is very straightforward to identify and mitigate. We assess the influence on the WIMAX/LTE network and the number of people who will be able to utilize it.

2) *A security vulnerability involving denial of services (DoS)*

DoS assaults are a concern for Wi-max networks. These assaults may be launched by launching a flood attack on legitimate organization frames.

3) *Problems with Wi-Fi security*

For more than a decade, wireless LANs based on WI-FI technologies have been obtainable. The Wi-Fi, on the other hand, was a disappointment. Most people use technology in their homes and in public locations like airports, hostels, and retail malls. Although the cost advantages of Wi-Fi may be appealing to businesses, if security is clear, it is less harmful because of increased mobility, lower operating expenses, and flexibility. As a result, safety experts to create it appropriate to the company, have concentrated on security coercion as well as solutions in the context of Wi-Fi networks, the original Wi-Fi security solution, had a number of security measures. Problems caused by poor encryption, such as using the RC4 stream cipher with CRC-32 authentication.

4) *Potential 4G Threats*

The 4G network may confront a slew of potential safety issues. The infrastructure is accessed through a variety of heterogeneous technologies, therefore to safeguard technology, feasible security is required. It also has the potential to bring the whole network architecture down if too many people use it. The basic network infrastructure is distributed across service providers. End-user equipment may potentially become a problem with 4G wireless[10], [11].

Worms, malware, phone calls, and spam emails, among other things, are a source of malicious assaults. Spam on the internet is the new spam. VoIP has resulted in a serious issue, similar to today's e-mail junk. As with the previous VoIP terrorizations, there are three additional VoIP dangers.

- Spoofing, which misdirects transportation, alters data, or transfers money using a stolen credit card information, is a threat.
- Typical input point hijacking, in which the attacker's IP address is substituted for the packet header's IP address.
- Dropping IP packets are intercepted and encrypted as part of a secret transaction.

F. Difference between 4G and 4G LTE

The distinction between 4G and 4G LTE is mainly about marketing and the 4G specification's history. LTE (Long Term Evolution) was created to enable the transition from 3G to 4G simpler for providers. The International Telecommunication Union (ITU) originally defined 4G in 2008, but its speeds and technical requirements were not immediately available for mobile networks or devices. LTE delivers greater bandwidth than 3G as a step up from 3G, but without hitting the full bandwidth network speed minimum of 100 Mbps that 4G promises. The word LTE is often used in marketing presentations, however it does not indicate or identify a particular speed. Speeds vary from 20 Mbps to 100 Mbps, depending on the provider. However, 4G LTE-A (LTE-Advanced) is a special word that means it can provide speeds of up to 100 Mbps. It is, in essence, 4G, with no technological differences.

II. DISCUSSION

The use and implementation of the online electronic system is now increasing at a quicker rate. Data or information supplied over the network must be secure, particularly in the financial industry, online shopping platforms, and personal data Logging systems, for example. This section goes through many different forms of security attacks. The majority of the communication medium is open and available to everybody, however network jamming and femtocells are still difficulties. The protection of personal information is paramount. When cellular devices transfer data through radio transmission, the attacker will receive it disrupt the channel of communication Jamming is the act of interfering with these signals. It is feasible to jam a wide spectrum of frequencies. Security rules must be controlled by the home operator, and security solutions must not obstruct service delivery or handovers in a manner that is obvious to end users. In addition, the EPS must offer various degrees of proper user privacy for communication, location, and identification. The communication's content, origin, and destination must all be specified.

Despite the fact that 3G has yet to be completely deployed in the real world, many have begun to discuss the benefits of 4G. QoS and mobility are two of the 4G services that have been discussed. There's also the idea of always best connected, which implies the terminal will always choose the best available connection. The IPV6 address system will also be used in 4G. Each cell device may be able to have its own IP address as a result of this. Currently, the challenge of security is addressed by using many levels of protocol stack encryption. This technique has drawbacks such as wasted power, lost energy, and a longer transmission latency. In 4G, the notion of interlayer security will be used, with just one layer set to encrypt data. For high-speed wireless data transfer, 4G networks have been employed all over the globe. The extensive use of the technology drew the attention of the hacker community, who sought to steal and misuse data. The volume of personal and sensitive data sent across the internet raises security concerns.

A. *Impact of LTE's*

- 3GPP designed the 4G LTE architecture with security principles in mind from the start, with five security feature groups to choose from [2].
- Network domain security, which protects network components while also securing signaling and data transmission between users.
- Controlling safe access to mobile stations through the user domain.
- Applications area security, which ensures secure communication at the application layer.
- Security visibility and configuration allow users to verify whether security features are active.

B. *Secure Option*

There is hope since there are a few choices for connecting to the Internet using your mobile smartphone. When it comes to public Wi-Fi, attackers have more opportunity to exploit vulnerabilities via Wi-Fi than they do over 4G. Here's how these connections rank in terms of security, from most secure to least safe:

- Using a VPN over a cellular network or a VPN over a public Wi-Fi network
- Only cellular
- Only Wi-Fi is available.

Using a multi-layered strategy is the best method to maintain your security when on the road. Anti-malware software, firewalls, VPNs, and online common sense are all essential.

III. CONCLUSION

MNOs play a key role in LTE network security via design, implementation, and operations, regardless of the fact that the 3GPP has created a robust security architecture for 4G LTE. MNOs can't afford to disregard LTE security, and they must constantly monitor the network's various access points. Despite the fact that 4G LTE contributes to the difficulty of MNO security management, MNOs can limit the effect of various security concerns with appropriate attention. To keep up with the evolving threat environment, security is generally acknowledged as a moving target that requires constant attention and investment. When 4G LTE services and technology are implemented, security will become an even more important part of MNOs' business lifecycle.

Despite the fact that the 3GPP has built a comprehensive security architecture for 4G LTE, MNOs play a vital role in LTE network security management via design, deployment, and operations. MNOs can't afford to ignore LTE security, and they need to keep an eye on the network's numerous access points at all times. Regardless of the fact that 4G LTE adds to MNO security management's complexity, MNOs may mitigate the impact of numerous security risks by paying attention to them. Security is widely accepted as a shifting target that needs continual attention and effort to stay up with the developing threat landscape. Security will become an even more significant aspect of MNOs' business lifecycle once 4G LTE services and technologies are introduced. As a result, 4G networks will face more security concerns than current-generation networks. Users were able to extend their businesses and connect globally thanks to customized versions of these cellular networks. As the usage of communication has progressed from a personal to a professional level, the growth of 4G has offered professionals with a time-saving and easy-access technology. New dangers and assaults will continue to emerge as security evolves. As a consequence, a comprehensive threat analysis and the development of appropriate countermeasures for the whole 4G system must be carried out concurrently with the growth of 4G architecture, which is now being investigated.

REFERENCES

[1] S. K. Mohapatra, B. R. Swain, and P. Das, “Comprehensive Survey of Possible Security Issues on 4G Networks,” *Int. J. Netw. Secur. Its Appl.*, 2015, doi: 10.5121/ijnsa.2015.7205.

[2] A. N. Bikos and N. Sklavos, “LTE/SAE security issues on 4G wireless networks,” *IEEE Security and Privacy*. 2013, doi: 10.1109/MSP.2012.136.

[3] R. M. Zaki and H. Bahjat Abdul wahab, “4G Network Security Algorithms: Overview,” *Int. J. Interact. Mob. Technol.*, 2021, doi: 10.3991/ijim.v15i16.24175.

[4] A. Singla, S. R. Hussain, O. Chowdhury, E. Bertino, and N. Li, “Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks,” *Proc. Priv. Enhancing Technol.*, 2020, doi: 10.2478/popets-2020-0008.

[5] A. Deshpande and D. S. Pawar, “Evolution of Wireless Technology,” *Int. J. Comput. Sci. Mob. Comput. IJCSMC.*, 2020.

[6] M. Meraj, I. Mir, and S. Kumar, “Evolution of Mobile Wireless Technology from 0G to 5G,” *Int. J. Comput. Sci.*

Inf. Technol. , 2015.

[7] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*. 2018, doi: 10.1016/j.jnca.2017.10.017.

[8] S. Farhan, M. Ali, M. Kamran, Q. Javaid, and S. Zhang, "A Survey on Security for Smartphone Device," *Int. J. Adv. Comput. Sci. Appl.*, 2016, doi: 10.14569/ijacsa.2016.070426.

[9] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks," *J. Netw. Comput. Appl.*, 2018.

[10] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," 2018, doi: 10.14722/ndss.2018.23313.

[11] D. Candal-Ventureira, P. Fondo-Ferreiro, F. Gil-Castiñeira, and F. J. González-Castaño, "Quarantining malicious iot devices in intelligent sliced mobile networks," *Sensors (Switzerland)*, 2020, doi: 10.3390/s20185054.