e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707258 |

Potential Security Concerns for Upcoming Mobile Wireless Networks

Ranjitha.T, Prof. Mahendra Kumar B

MCA Student, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

Professor, Dayananda Sagar College of Engineering, Bengaluru, Karnataka, India

ABSTRACT: When 5G wireless networks for smartphones finally arrive, many will be concerned about their safety. It is imperative that we thoroughly evaluate the new 5G wireless mobile network in comparison to the older 4G cellular network. The article begins by outlining the 5G network's objectives, new requirements, and unique features with regard to mobile security. Possible dangers and security issues need our attention. Finally, security services are the foundation of the current 5G mobile network strategy. These services include device authentication, network availability within a defined area, data privacy and confidentiality, intrusion detection, and more. The integration of several state-of-the-art technologies, such as the Internet of Things (IoT) and massive multiple-input, multiple-output (mMIMO), into 5G mobile wireless networks has improved security. Here, 5G mobile wireless networks, intrusion detection systems (IDS), and 5G security are all interdependent.

KEYWORDS: Firebase, Android, Java, Application, Notification, College, Events, Management, Mobile.

I. INTRODUCTION

The most recent iteration of mobile communication networks is known as 5G, or Fifth Generation Wireless System. It goes much beyond being only the most recent version of the 4G networks that are now operational. to a much greater extent. It will introduce new service capabilities and create problems with their worldwide deployment. By 2020, there will be more mobile devices in use than ever before, leading to a dramatic spike in data traffic compared to the present [1]. 5G mobile telephony is necessary since the existing cellular network, 4G, cannot satisfy these expectations. In addition to cutting-edge services like Device-to-Device (D2D) communication, massive Multiple Input Multiple Output (mMIMO), and dense network devices with capacities higher than 4G, the researchers will be concentrating on a plethora of other technologies. Specifically for 5G's advanced features, we aim for: connections between 1 and 10 Gbps; devices linked to the network that are 10 to 100 times more powerful than the current system; availability of the network at almost 100%; power consumption of the network reduced by 90%; and battery life for devices with lower power consumption extended to up to 10 years. 5G also makes use of other technologies to achieve these goals, including as the network. The atmosphere is filled with a mixture of excitement and anxiety as we get closer to the beginning of the change brought about by mobile technology. The next generation of mobile wireless networks, which will include 6G and other generations, will provide innovative new capabilities, connections that are unmatched, and speeds that are Lightning fast.The designations mmwave, HetNet, mMIMO, direct-to- device (D2D), and machine-to-machine (M2M) denote several categories of wireless communication. In essence, 5G wireless technology (Figure 1) [2] displays the systems in action. 5G will not only deliver improved telecommunications and internet capabilities, but also other advancements. However, it has specific applications in smart cities, healthcare, industrial automation, and vehicle-to-vehicle communication. The emergence of state-of-the-art technology, architecture, and applications brings up a multitude of new security considerations. Future mobile wireless networks need novel intrusion detection techniques. Considering the fact that the 5G network will be diverse [11], The current mechanisms are ineffective in providing security . Due to limited capacity and broadcast transmission style of modern wireless communication, providing security to users is both possible and difficult.

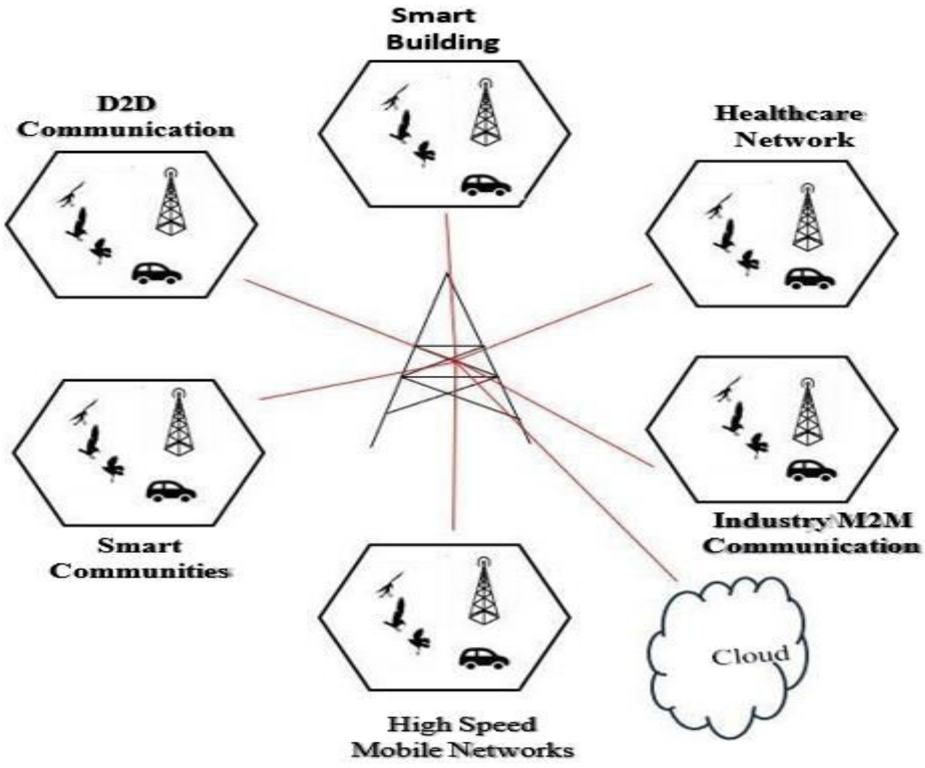
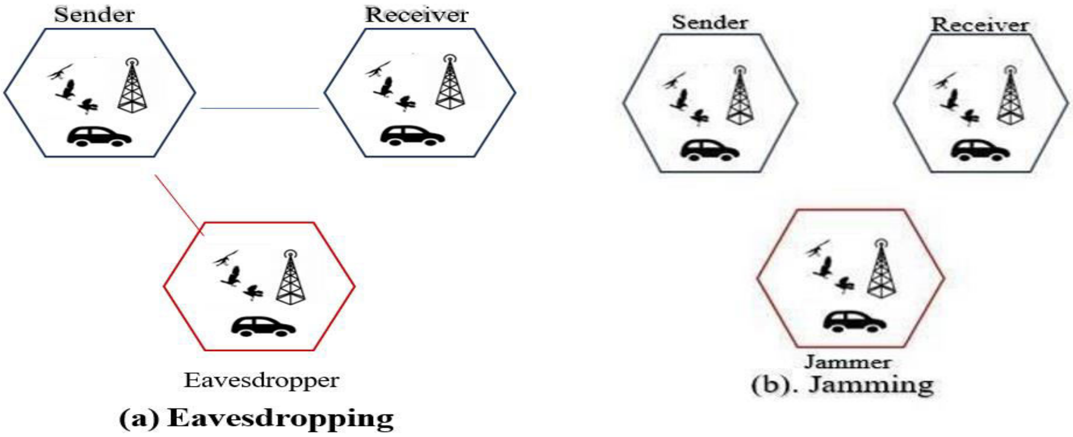


Fig. 1. General Architecture Of 5G Wireless System.

II. VIRUSES IN THE 5G NETWORK



(a) Eavesdropping

(b). Jamming

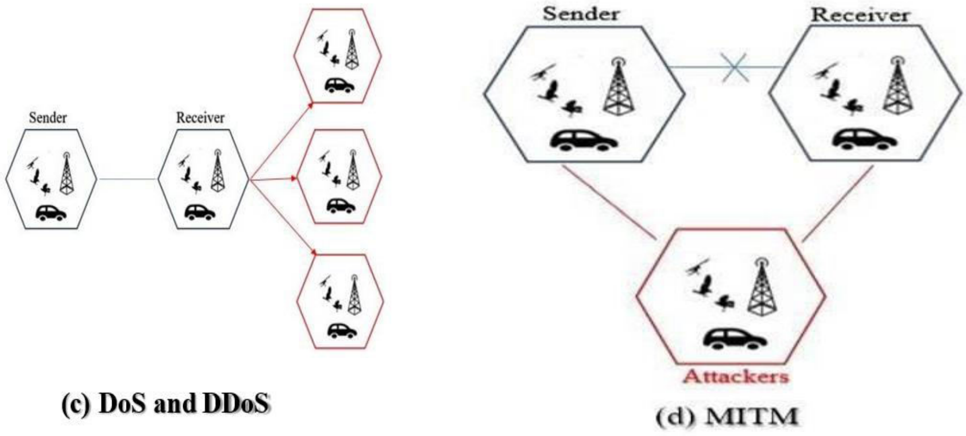


Fig. 2. Viruses in the 5G Network

The attacks as depicted in Fig. 2, and each is described by thoroughly considering both the attack and the security measure [2].

As there isn't any interference with the network or communication, traffic monitoring and analysis is considered a passive assault. In this kind of assault, the criminal secretly listens in on two legitimate users. Due to its passive nature, this assault often passes unnoticed. Encryption methods make it difficult for an eavesdropper to decipher an encrypted transmission, protecting it against these types of attacks. Communication patterns, party identities, and location data may be intercepted by attacks that employ traffic analysis. Even when a message is encrypted, a traffic analyzer can still decipher the transmission pattern. Networks and communication are also unaffected by these attacks. Data confidentiality and user privacy are breached by these assaults.

The effectiveness in terms of encryption mechanism is of utmost importance in thwarting such attacks; otherwise, the communication may be easily deciphered by the eavesdropper, who may be using more powerful equipment than the conversing parties. The existing method of eavesdropping depends on the eavesdropper's restricted processing capacity and data analyzing abilities. In addition, more difficult circumstances may arise because some technologies, such as the Internet of Things and HetNet, may struggle to prevent eavesdropping. 5G gives greater weight on PLS techniques than cryptography when trying to solve these problems [9].

B. **Jamming:** unlike issue previously mentioned, jamming has the ability to totally halt communication between authorized users. Jamming stops authorized users from interacting with others and using radio resources. This kind of attack is active, and the response to an active attack is focused on detection. Better error rate performance and faster detection times can be achieved by preventing these kinds of attacks with the help of a resource allocation approach. Malicious nodes, as seen in the figure, prevent two authorized parties from communicating [9].

C. **DoS and DDoS:** It is possible that a prospective eavesdropper, who may be armed with more sophisticated technology than the people involved, could quickly interpret the conversation if the encryption mechanism does not have sufficient strength. As stated to the current eavesdropping technique, the method's efficiency is contingent on the eavesdropper's processing and data analysis capacity, which may not always be sufficient. Some technologies, like HetNet and the Internet of Things, incorporate vulnerabilities that enable eavesdropping, adding an additional layer of complexity to the problem. 5G networks prioritize PLS approaches over encryption to address these issues [9].

D. **MITM**: In a man-in-the-middle assault, an adversary takes control of the user-to-user communication. It is convensible that the attacker may completely replace, modify, or otherwise alter the message that is going to be transferred between two parties. people getting together. There are simulations of MITM attacks shown in Figure 2. In addition to this, continuing assault that constitutes a threat to the availability, integrity, and privacy [9].

III. SECURITY SERVICES

Furthermore, introducing new capabilities, new situations, new technology, and extra alternatives, 5G wireless networks also provide new security concerns. Integrity, availability, confidentiality, authentication, and intrusion detection are the five aspects of security services that are discussed in this article.

A. Authentication: When considering to authentication, the main types are: message authentication and entity authentication [2]. So that one has to protect users' privacy and avoid the aforementioned risks, these authentications are essential. In 4G LTE, authentication between smartphones and base stations is a must to any connection. At the moment, cellular networks employ symmetric key authentication 5G. Alternatively speaking, facilitates talk between non-UE users as well as UEs and base stations.

B. Confidentiality: Both personal information and sensitive data are subject to different levels of secrecy [2]. Keeping data confidential is one line of defense against passive assaults. Users cannot analyze or manipulate data if unauthorized access is present. Looking at someone's travel habits is one way to ascertain their whereabout or other private information. This is quite delicate the substantial volume of confidential data that 5G will transmit, which consist data from different apps and data. The most common application of cryptographic methods for data secrecy is to prevent hackers from accessing data. Both the originator and the receiver use secret key encryption, either called as symmetric key encryption, to encrypt and decrypt data. The two participants in this cryptosystem should share the private key. A secure key distribution technique accomplishes key sharing. Prior methods assumed that the adversary had less sophisticated hardware and computational capabilities. Therefore, such strategies fail when faced with adversaries who possess superior computing capabilities. Based on conditions, PLS may provide an improved defense against assaults that use jamming and eavesdropping.

C. Availability: Availability refers to a service's capacity to be accessible and utilized by users, irrespective of their location or time of day [2]. It may also indicate how well a service can withstand any kind of attack. Delusional and distributed denial-of-service attacks jeopardies network availability. Jamming may hinder communication among authorized users by disrupting their communication channels. As many Internet of Things networks increases, it will become more challenging to maintain the security of 5G wireless networks against denial-of-service and jamming attacks. A successful plan is needed for addressing these issues is to allocate resources

D. Integrity: While message authentication guarantees the sender's authenticity, it doesn't guard against message alteration or duplication. 5G wireless networks target to be accessible for large group of people for life-related applications like car and health monitoring and efficient use of the network. The most important aspects of 5G security is data integrity. No one can tamper with or duplicate the message if it has integrity [2].

E. Intrusion Detection: Modern society nevertheless faces serious challenges when it comes to security, despite the existence of the aforementioned measures to avoid invasions [11]. Important considerations include getting around security mechanisms such as authentication.

IV. 5G TECHNOLOGY UTILIZED

Here we see the many different kinds of technology that 5G wireless networks may utilize . We'll take a cursory see the novel possibilities and uses for these emerging technologies.

A. **HetNet:** HetNet is the best high-coverage 5G service. Furthermore, among its other diverse attributes, HetNet provides the best coverage, high capacity, energy efficiency (EE), and spectrum efficiency (SE) performance measures. Despite these enhancements, HetNet is still more vulnerable to eavesdropping on user equipment compared to previous, single-tier networks. Due to its dense architecture, HetNet's handover performance will degrade if small cell handover occurs too frequently. [2]

B. D2D : Direct-to-device (D2D) communication allows devices to link up without going through a base station. D2D communication allows for efficient spectrum utilization. It also helps lighten the burden on Base Station. Dynamic spectrum access, while commonly employed to improve spectrum efficiency, opens the door to attacks like jamming. Allocating resources through cooperation between D2D nodes is the most preferred way to safeguard D2D communication. Collaboration, channel access, and power control can achieve D2D communication security [7].

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707258 |

C. Massive MIMO: Extensive use of antennas can enhance the energy and spectrum efficiency of the network. In addition, it has the potential to enhance network security; nevertheless, the large antennas will cause significant interference and result in inconsistent performance. Here we meet beam creation, yet another technological advancement. Large MIMO systems, however, are vulnerable to eavesdropping assaults. In this regard, using PLS in 5G networks may be critical [8].

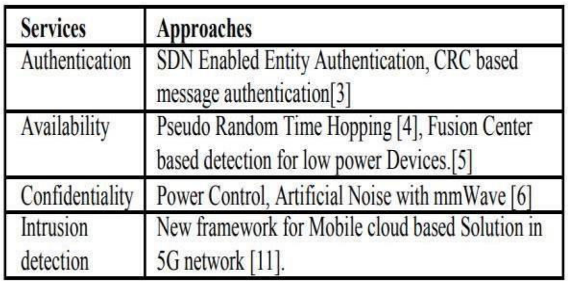
D. Internet of Things: In the many of the cases, IoT nodes aren't very powerful and don't have much processing capacity. With so many restrictions on their power and computing capabilities, it becomes difficult to ensure the safety of these nodes. An efficient and lightweight security solution is required. Relaying is a widely used and efficient approach to addressing these difficulties. The IoT utilizes RFID, which represents radio frequency identification. RFID technology has several pragmatic applications, such as facilitating inventory management and automating traffic flow. The IoT is a very promising technology that is rapidly expanding and necessitating more robust networks.

E. Intrusion detection techniques: A wired network often uses two layers of protection. First is setting up a firewall at the gateways. Later set up devices such as routers and switches, followed by a system that detects intrusions when malicious data tries to enter the network and manages to bypass the firewall. Nevertheless, in light of the potential future of mobile wireless networks, it is essential that each node include a security mechanism. Every end user must install an intrusion detection system because not all networks are the same. Security is of utmost importance due to its potential consequences of bypassing the aforementioned safeguards, such as authentication. This make use of either new or preexisting IDS frameworks or methods will be required [11].

V. OBSERVATION AND EXISTING WORK

Despite the substantial progress in creating 5G, the process of developing defined protocols is still in its early stages. Depending on the circumstances, being a part of this young and developing technology could go in million of different directions. The table below provides a thorough outlook of the measures that could significantly improve the security and reliability of communication in 5G networks. This article presents a limited selection of the many innovative methods available. We must dedicate a significant amount of effort, specifically considering field of intrusion detection techniques, to ensure security.

TABLE I Different services and approaches in 5G



Services	Approaches
Authentication	SDN Enabled Entity Authentication, CRC based message authentication[3]
Availability	Pseudo Random Time Hopping [4], Fusion Center based detection for low power Devices.[5]
Confidentiality	Power Control, Artificial Noise with mmWave [6]
Intrusion detection	New framework for Mobile cloud based Solution in 5G network [11].

VI. CONCLUSION AND FUTURE

So far research on the 5G network has shown that it is an advancement over previous networking technologies that offers a wealth of new opportunities. This report provided a concise summary of the latest research on 5G wireless networks. Availability, authentication, data confidentiality, and integrity are just a few of the many security-relatedsubjects we have covered. Different security scenarios have been considered as a result of the deployment of technologies such as HetNet, IoT, mMIMO, D2D, and intrusion detection approaches. A lot of effort will be required in this area since new security needs will emerge as a consequence of various new prospects and technical advances.
The 5G mobile is quite diverse, which has led to the introduction of many new technologies. We will also conduct in-depth investigations into several novel applications of technology. Because of this, future mobile wireless networks that use network slicing, software-defined networks, network function virtualization, mobile cloud computing, or ad hoc networks to identify intrusions may face more challenges.

REFERENCES

1. "6G Security: A Survey on Authentication, Privacy, and Key Management" by J. Li et al. IEEE Communications Surveys & Tutorials, 2023.
2. "Blockchain-Based Identity Management for the Internet of Things in 5G and Beyond Networks" by Y. Li et al. IEEE Network, 2021
3. "Security and Privacy for Non-Terrestrial Networks in 6G: Challenges and Opportunities" by Q. Wu et al.IEEE Wireless Communications, 2023.
4. "Artificial Intelligence-Assisted Security for Future Wireless Networks: Opportunities and Challenges" by H. Zhang et al. IEEE Wireless Communications, 2023.
5. “Physical-Layer Security Techniques for Emerging Millimeter-Wave and Terahertz Wireless Networks" by Z. Zhou et al. IEEE Journal on Selected Areas in Communications, 2020
6. Software-Defined Networking Security for 5G and Beyond Mobile Networks" by M. Asim et al., IEEE Network, 2019.
7. "Resource Management and Security in Mobile Edge Computing for Industrial IoT" by S. Deng et al. IEEE Transactions on Industrial Informatics, 2023.
8. "Lightweight Authentication and Key Management Schemes for Delay- Sensitive Applications in Cellular IoT" by L. Zhou et al.IEEE Access, 2022.
9. "Secure Federated Learning for Collaborative Intelligence in Wireless Networks" by W. Sun et al.IEEE Transactions on Wireless Communications, 2023
10. "Blockchain-Based Trust Management for Device-to-Device Communications in 5G Networks" by M. Shah et al. (IEEE Transactions on Vehicular Technology, 2021)
11. "Machine Learning-Based Intrusion Detection in Mobile Edge Networks for 5G and Beyond" by Y. Wu et al. (IEEE Transactions on Network and Service Management, 2023)

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com