Analysis of the Security of 5G Technology from the Network Level

Lei Shi*

School of Computer Science, University of Leeds, Leeds, LS2 9JT, United Kingdom

ABSTRACT: In today's society, 5G network technology has gradually entered everyone's life, from the simplest communication to smart cars, artificial intelligence, traffic signals to the medical field, military industry and so on. All aspects of 5G network technology can be used to greatly improve the convenience of people's lives and the technological transformation of human society. However, there are many countries, companies and people who are not so sure about 5G technology, and who may even abandon its use because of concerns about its security. As a result, this thesis focuses on the benefits and drawbacks of 5G technology's security in networks, as well as its application in everyday life and potential security threats, as well as whether its security will escalate from a cyber-level attack to physical harm to humans or facilities when combined with the Internet of Things. The analysis of current articles, data, and expert opinion will help to produce findings that will address the concerns of those who are sceptical about the security of 5G. In this regard, it is concluded that the safety of 5G network technology requires a warning, but at this stage, its convenience and safety are within human control and can be used with confidence.

1. INTRODUCTION

As one of the more advanced technologies of today, 5G technology has an essential role to play in various fields. In its current form, the development of 5G technology has reached a stage where it is considered white-hot. It is being used in the fields of communications, healthcare, transport, satellites, and the military. However, in the process of developing technology, there are inevitably security issues associated with it. This paper focuses on the security aspects of 5G technology in the network and discusses the pros and cons of security in this area. Through the research in this paper, people will be able to understand more about the security of 5G living and be more confident and reassured about it. At the same time, it will provide advance warning of possible dangers and enable people in the field to avoid them. This paper focuses on the security of 5G networks, its principles and advantages and disadvantages, the security of applications in 5G networks, the different areas of application and the security analysis therein, as well as the threat of attacks at the network level to physical damage and cyber warfare to analyse and discuss the issues involved.

2. SECURITY OF 5G NETWORKS

2.1. Introduction to 5G network principles

The introduction of 5G networks is revolutionary. Its excellent transmission rates, stability and low latency are commonly understood features. Although the 5G network architecture is largely a continuation of the 4G network architecture, there are certain features of the 5G networking model and technology.

The 5G network architecture can be simply divided into four main components: terminals, access network, core network and applications. The 5G security report from the China Communications Research Institute points out that in this, new key technologies that are more innovative and could even revolutionize the network are used in both the access network area and the core network area [1].

The main key technologies here are service-enabled architecture, network function virtualization, network slicing, edge computing, network capacity opening and key technologies for the access network.

Since we mainly need to discuss security, we will talk in detail about edge computing technologies and access network key technologies.

Firstly, edge computing technology: this technology provides two major capabilities, one for computing and one for data processing, at the edge of the network and at two specific locations close to the user. Through these two capabilities, the overall network data processing efficiency is improved, as the data is not sure how large the application is at the time, so the efficiency can effectively meet some of the needs of low latency, high traffic, security, and stability.

Next is the key technology of the access network: this technology is to use a lighter and faster system design while using new channel coding schemes and larger scale antenna technology and other technologies to achieve high transmission rates and better [1].

*Corresponding author. Email: ml20l2s@leeds.ac.uk

It can therefore be seen that 5G technology is a leap forward compared to 4G technology and allows 5G network technology to be used on a much wider level.

2.2. 5G Cybersecurity Strengths and Weaknesses

Security is also a crucial issue in 5G networks, which includes the security of devices, applications, and other endpoints as well as the security of the network itself. It is also the importance of network security that makes 5G network technology of great interest in this area and will have its relative benefits and drawbacks.

2.2.1. Strengths

Compared to 4G, 5G offers a more robust security capability at the network level. Through the report of the China Academy of Information and Communication Research we can know that it contains service domain security, enhanced user privacy protection, enhanced integrity protection, enhanced inter-network roaming security, unified authentication framework, etc.

For the enhanced user privacy protection integrity protection, the 5G network has a more accurate processing capability in user identification, which can be based on the original 4G user data encryption protection, and more integrity protection to prevent data tampering and other situations.

2.2.2. Weakness

Shane Fonyi touches on the security issues for the AKA protocol in 5G. His article mentions that Cremers and Dehnel-Wild believe that the 5G-AKA protocol does not meet its security requirements. They show through their research that an attacker can use legitimate users other than themselves to access the operational network, making it unpredictable. When a device is roaming, the insecure transmission mechanism of keys used to transfer authentication between the terminal and the base station might lead to attacks. The absence of randomization in the sequence number in the current AKA standard for 5G has been found as a vulnerability that might allow an attacker to replay a user's cellular use (SON). As a result, the sequence number may be thought of as a pass that grants access to certain resources. As a result, the attacker would be able to learn about the other party's phone conversations, text messages, and other communications, as well as the duration of certain web traffic [2].

These seemingly small or insignificant attacks can have a significant impact on a person's privacy, and after repeatedly extrapolating the time and other information, it may be possible to get hold of some habits, behaviour, and even specific personal information of the attacker.

3. APPLICATION SECURITY ISSUES IN 5G NETWORKS

3.1. Areas of application for 5G use

The arrival of 5G has led to a degree of improvement in many areas of people's lives and has bred technological innovation in many areas. It will be studied from two main areas healthcare and artificial intelligence, as well as some other areas where the role of 5G is revolutionary and is greatly increasing the convenience involved.

3.1.1. Medical field

In this field, the low latency and high speed of 5G network technology can produce a qualitative improvement in all aspects of human health care. In addition to remote 5G surgery, which is well known, Dong LI mentions in his article that augmented reality (AR) and virtual reality (VR) are the areas of technology that are most likely to benefit directly from 5G technology, which can be easily applied to physical rehabilitation processes, as well as the ability to transmit important signals with almost zero latency (<1 ms radio latency, the error rate of minus 9 to the 10th power) precisely because they can be used for intuitive surgical training or even for the transmission of data. For more information, see Figure 1[3].

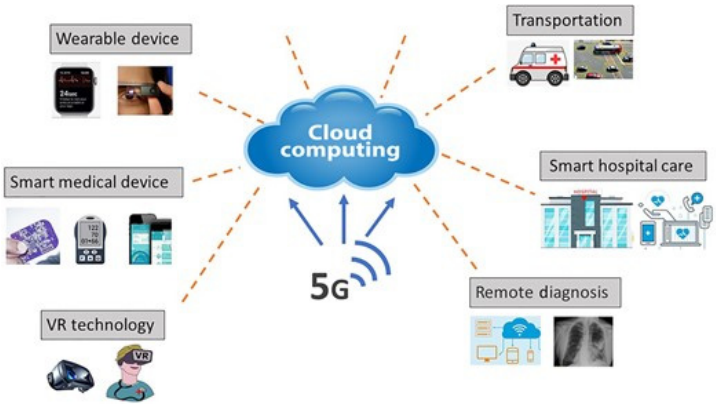

Figure 1. Cloud Computing

At the same time, the power of 5G is enabling many medical terminals to be technologically enhanced, for

example by enabling higher definition imaging systems, faster and more convenient medical communication systems, etc.

As a result, tele-medicine systems, in addition to virtual reality, are becoming more sophisticated and accessible with the arrival of 5G. The speed of 5G transmission is just one of the many advantages over 4G, but it is also a new interactive medical experience with ultra-low latency intervention and no network congestion. With effective tools and 5G networks, medical professionals who are far away or who are not easily able to travel can achieve the feeling of being there, effectively reducing the time delayed by distance.

3.1.2. Artificial intelligence field

In addition to medical applications, the use of 5G network technology in other areas is widespread and active.

Some of its applications for artificial intelligence are mentioned by Yasmin Tadjdeh in Defence, where Lindsey R. Sheppard, an Associate Fellow in the International Security Program at the Center for Strategic and International Studies (CSIS), presents Many examples of applications. For example, defence systems can profit from the Al capabilities afforded by 5G networks for military operators operating drone fleets, even though military lines are distinct from commercial lines. She tells out that, in addition to minimal latency, the benefits of 5G technology include high bandwidth and many data qua platforms for transmission. She believes that data processing and the facilitation of some terminals will have a big influence on artificial intelligence systems [4].

3.1.3. Other areas

In addition, 5G network technology will also be of great help in issues such as driverless technology, live broadcast technology and high signal coverage. As seen in the publicity for the 2022 Winter Olympics in Beijing, 5G events can be effectively broadcast in high definition and smoothly on high-speed trains at speeds of 350km/h.

Thus, 5G network technology is no longer just about the internet, it has gradually spread to all aspects of people's lives and is used to facilitate their lives.

3.2. Safety analysis in application areas

Because 5G applications are so numerous, it has often been the target of unsuspecting people. Firstly, the security threats in 5G applications are identified in articles by authors such as Qin Qiu and Shenglan Liu.

3.2.1. Main security threats

The device, network, edge, cloud, and centralized security operations and maintenance are the primary security threats for 5G applications in general, as indicated in Figure 2 [5].

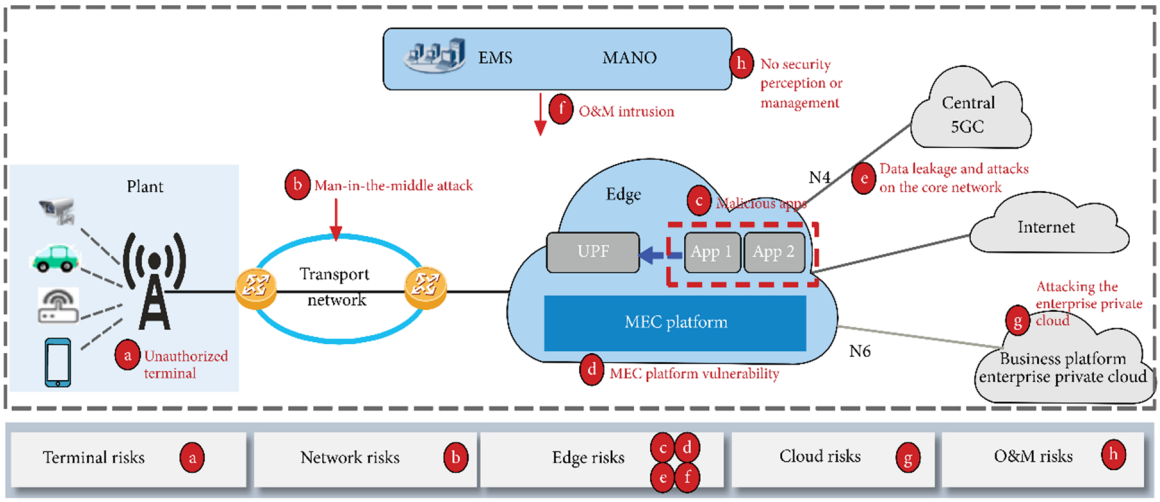

Figure 2. Risks to 5G applications in an end-to-end view.

First, unauthorized terminal access, abuse of authorised SIM cards, and attacks on and control of authorised terminals are all major security issues on the terminal side. Secondly, network slice isolation, misuse of slice resources, and theft and modification of user-facing information are all major security issues. Then, vulnerabilities in the MEC platform, untrusted apps on the MEC, and attacks on the MEC from the Internet, business cloud, and OM plane are all security issues on the edge MEC side. Then, MEC-based assaults on the workplace intranet, as well as theft or alteration of enterprise communications, are security vulnerabilities on the enterprise private cloud. Last, failure of security situational awareness, unified administration of security devices and policies, and a lack of O&M audits are all hazards from an O&M standpoint [5].

3.2.2. Three main areas

There are three main typical usage scenarios in which there are risks and security issues for those who use 5G.

3.2.2.1. eMBB scenario

The first is the eMBB scenario, which is concerned with bandwidth-intensive applications. Currently, the main forms of eMBB applications are 4K/8K HD video and mobile roaming immersive services based on virtual reality (VR) and augmented reality (AR), where security threats mainly include the failure of monitoring means resulting in eMBB applications generating large amounts of traffic, which can make it difficult for security devices such as firewalls and intrusion detection systems deployed in existing networks to provide adequate security protection in terms of security protection. radio This makes it difficult for security devices such as firewalls and intrusion detection systems to provide effective security protection in terms of traffic detection, radio coverage, and data storage when installed in existing networks [6].

Second, the privacy of users is jeopardised. User privacy information, such as personal information or identity, device identification, address information, and so on, is stored in a huge quantity of eMBB services (e.g., VR/AR). The open nature of 5G networks makes it more likely for personal information to be leaked [7].

3.2.2.2. uRLLC scenario

The second is in the uRLLC scenario. uRLLC is primarily focused on latency-sensitive services or applications, such as autonomous/assisted driving, remote control, industrial internet, and so on. The need for low latency and great dependability is critical. For example, if the vehicle network is exposed to a communication security issue, it might be life-threatening. As a result, uRLLC services necessitate a high level of security while avoiding any additional communication delays.

DDoS assaults are the most serious security threat. DoS/DDoS attacks can cause network congestion or communication outages, which can lead to service failure.

Attackers tamper/forge/replay application data by exploiting device and protocol vulnerabilities in the network data transmission channel (5G airports, core network, internet), leading to lower data transmission reliability and jeopardising proper application functionality [8].

3.2.2.3. mMTC scenario

The last scenario is mMTC. The 5G mMTC scenario supports IoT applications such as smart transportation, smart grids, smart cities, and other massive device interconnections. Because of its low cost, large-scale deployment, and limited resources, the following security flaws are frequent in IoT devices (e.g., processing, storage, and energy) [9].

Counterfeit endpoints are the first. Endpoints on the Internet of Things have limited resources and processing computational capacity. As a result, it's probable that authentication will be skipped or that basic techniques will have to be employed, opening the door for counterfeit endpoints, and causing uncertainty in the functioning of IoT applications [10,11].

Attackers can tamper with application data by exploiting flaws in endpoints and cloud/edge systems. In some sensitive areas such as banks, enterprises, etc., even very small changes through the tampering and falsification of critical data can have incalculable consequences.

Data eavesdropping User privacy is compromised by data acquired by IoT endpoints installed in certain contexts (e.g., the house, the medical environment). Weaknesses in the data transmission channel may result in user privacy being compromised.

Making use of a remote control. Attackers can take advantage of the simplicity of use and lack of security of IoT endpoints to remotely access and manage them via hardware and software interfaces, then use the captured endpoints to launch cyber-attacks [12-16].

As a result, it's clear to understand how 5G network technology's ease will be accompanied by a matching degree of security concerns and dangers.People may not realise it right now due to the continual debugging by many programmers or employees, but there are security issues that need to be addressed.

4. NETWORK LEVEL ATTACKS TO PHYSICAL DAMAGE

4.1. The physical threat of 5G networks under the IoT

The difference between 5G networks and 4G networks is not just in the block download speeds and smoother movie and video viewing but in the use and application of multiple fields. When 5G is combined with artificial intelligence and the Internet of Things, the results will be revolutionary. But at the same time, the security risks involved can be fatal. If an attack on a 4G network is the loss of signal, personal information, personal or business data, then with AI and IoT, an attack on a 5G network will cause harm to people, such as smart cars, national-level industrial facilities, etc.

During his speech at the first World 5G Conference, 350 Group Chairman and CEO Hongyi Zhou said, "In the future, through 5G networks and the Internet of Things, all network attacks can become physical damage, and many hackers with national backgrounds and national forces are starting to enter" [17].

In other words, unlike previous cyber-attacks, there will not only be individual 'petty' attacks, but also commercial, enterprise, and even national level attacks.

4.2. Coping with cyber warfare in the 5G era

In the face of difficulties and security threats, there is no need to panic excessively, but you can seek some good, upgraded solutions that can also be solved.

If we are now security or the old three: antivirus software, firewall, intrusion detection, which is almost ineffective for network warfare, if the potential attack or

latent attackers see are invisible, there is no way to defend, no way to block, Hongyi Zhou week that, first and foremost, to solve the "see" problem, if we are now security or the old three: antivirus software, firewall, intrusion detection, which is almost ineffective for network warfare, if the potential attack or latent attackers Consequently, he proposed Big data is the only way to look at it. Because all network assaults leave traces on mobile phones, laptops, and IoT devices at some point. The key to tackling the problem of network attack and defence in the 5G age is to use security big data to construct a radar for the network era, which can detect network attacks such as stealth planes [17].

In fact, attacks exist in the shadows, and it is difficult to know the identity of the attacker, perhaps as opposed to some governments or businesses that choose to face these as a process of stepping out of their comfort zone. It may be difficult to accept 5G because of interest, because of conservatism, because of unease, but if one is willing to accept 5G as one accepted 4G, then from the present process to the full entry into the 5G era, the world will take greater and greater steps and will reach its goal sooner and sooner.

5. CONCLUSION

The analysis shows that 5G network technology has a good aspect of security, with more stable transmission, faster speeds and lower latency compared to 4G. The main areas that need to be improved include the problem of attacks by attackers. So, in fact, the strength of 5G lies in its own security, while the weakness lies in attacks by other elements or people outside of it. But in fact, one can rest assured that in the three years that have passed since the World 5G Congress, 5G has come into our lives and has successfully made the transition to life, whether in transport, healthcare, the military, etc. and especially in the field of communication, which we are using. The benefits are very insignificant in the face of the technological innovations of human civilisation, so if more and more people or governments can embrace, improve and continuously explore the development of 5G network technology, the benefits will definitely be for the society and all the people. There are still some shortcomings in this paper in terms of data research, which can be improved by adding more first-hand research in the future. Future research will focus on the security applications and analysis of 5G in the IoT domain.

ACKNOWLEDGMENTS

First, I would like to thank my school, the University of Leeds, where my expertise in computer science helped me a lot and got me interested in this area. Secondly, I would like to thank my dissertation teacher, MS Huang, for helping me a lot with the literature search website and some formatting issues. Finally, I would like to thank myself for the countless days and nights I could keep studying and improving to finally finish this partial thesis.

REFERENCES

1. IMT-2020 (5G) Promotion Group 2020. 5G Security Report. China Academy of Information and Communications Technology.
2. Fonyi, S. 2019. Overview of 5G Security and Vulnerabilities. International Conference on Cyber Conflict (CyCon U.S.). Vol.5(No.1), pp.117–134.
3. Dong, L. 2019. 5G and intelligence medicine—how the next generation of wireless technology will reconstruct healthcare? Precision Clinical Medicine. 2(4), pp.205–208.
4. Tadjdeh, Y., 2019. 5G wireless network could revolutionize AI. National Defense Vol. 103, 9–1. https://doi.org/https://www.jstor.org/stable/27022425
5. Qiu, Q., Liu, S., Xu, S. and Yu, S. 2020. Study on Security and Privacy in 5G-Enabled Applications. Wireless Communications and Mobile Computing. 2020, pp.1–15.
6. CAICT, IMT 2020(5G), Promotion Group, 5G Security Report, The China Academy of Information and Communications Technology (CAICT) and IMT 2020(5G) Promotion Group, 2020.
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, vol. 101, pp. 55–82, 2018.
8. S. Basudan, X. Lin, and K. Sankaranarayanan, “A privacy-preserving vehicular crowdsensing-based road surface condition monitoring system using fog computing,” IEEE Internet of Things Journal, vol. 4, no. 3, pp. 772–782, 2017.
9. K. Fan, Y. Gong, C. Liang, H. Li, and Y. Yang, “Lightweight and ultralightweight RFID mutual authentication protocol with cache in the reader for IoT in 5G,” Security and Communication Networks, vol. 9, no. 16, 3104 pages, 2016.
10. D. Wang and P. Wang, “Two birds with one stone: two-factor authentication with security beyond conventional bound,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 4, pp. 708–722, 2018.
11. D. He, D. Wang, and S. Wu, “Cryptanalysis and improvement of a password-based remote user authentication scheme without smart cards,” Information Technology and Control, vol. 42, no. 4, pp. 170–177, 2013.
12. GTI, 5G Network Security Consideration White Paper v1.0, GTI, 2019.
13. ENISA, Threat Landscape for 5G Networks, European Union Agency for Network and Information Security (ENISA), 2019.
14. X. Ji, K. Huang, L. Jin et al., “Review of 5G security technology,” Mobile Communications, vol. 43, no. 1, pp. 40–45+51, 2019.

15. D. Wang, C.-G. Ma, Q.-M. Zhang, and S. Zhao, “Secure password-based remote user authentication scheme against smart card security breach,” Journal of Networks, vol. 8, no. 1, pp. 148–155, 2013.
16. D. Wang, X. Zhang, Z. Zhang, and P. Wang, “Understanding security failures of multi-factor authentication schemes for multi-server environments,” Computers & Security, vol. 88, p. 101619, 2020.
17. Zhang, H. 2019. Hongyi Zhou warns of 5G era: all cyber-attacks could turn into physical damage. China Economic Network. [Online].