Journal of Digital Convergence
Vol. 17. No. 12, pp. 197-202, 2019

ISSN 1738-1916
https://doi.org/10.14400/JDC.2019.17.12.197

Security Vulnerability and Countermeasure on 5G Networks: Survey

Sunghyuck Hong
Professor, Baekseok University, Division of ICT

5G 네트워크의 보안 취약점 및 대응 방안: 서베이

홍성혁
백석대학교 ICT학부 교수

Abstract In line with the era of the 4th Industrial Revolution, 5G technology has become common technology, and 5G technology is evaluated as a technology that minimizes the speed and response speed compared to 4G using technologies such as network slicing and ultra-multiple access. 5G NR stands for 5G mobile communication standard, and network slicing cuts the network into parallel connections to optimize the network. In addition, the risk of hacking is increasing as data is processed in the base station unit. In addition, since the number of accessible devices per unit area increases exponentially, there is a possibility of base station attack after hacking a large number of devices in the unit area. To solve this problem, this study proposes the introduction of quantum cryptography and 5G security standardization.

Key Words : Network Slicing, Base station, Quantum Cryptography, Standardization, Process

요 약 4차 산업혁명시대에 발맞춰 통신 기술도 5G 기술이 보편화되고 있으며, 5G 기술은 네트워크 슬라이싱, 초다접속 등의 기술을 이용해 4G에 비해 빠른 속도와 응답 속도를 최소화한 기술로 평가 받고 있다. 5G NR은 5G 이동통신 표준을 의미하고, 네트워크 슬라이싱을 통해 네트워크를 병렬연결로 잘라 네트워크를 최적화한다. 또한 기지국 단위에서도 데이터를 처리하게 되면서 해킹에 대한 위험이 증가 되고 있는 실정이다. 또한, 단위면적당 접속 가능한 기기의 수가 기하급수적으로 늘어나므로 단위면적 내 기기 다수 해킹 후 기지국 공격 가능성 또한 존재한다. 이에 해결 방안으로는 양자암호통신 도입, 5G 보안 표준화 등을 본 연구에서 제안하여 안전성과 통신속도를 전부 만족시키는 방안을 제안한다.

주제어 : 5G, 네트워크 슬라이싱, 해킹, 기지국 공격, 양자암호통신, 표준화

1. Introduction

With the recent launch of the 5G service plan by telecommunication companies. Samsung has also launched the Galaxy S10 5G model, and 5G commercialization began in earnest. However, security issues are constantly arising in 5G technology. In particular, issues related to network slicing technology, chopper connection, and edge computing, which are considered to be core technologies of 5G, are mainly discussed.

With the development of 5G technology, the importance of security becomes even more important as not only the existing smart phones,

*This paper was supported by 2019 Baekseok University Fund.
*Corresponding Author : Sunghyuck Hong(sunghyuck.hong@gmail.com)
Received September 16, 2019 Revised October 20, 2019
Accepted December 20, 2019 Published December 28, 2019

computers, but also things around us can be connected to the network. Although the features of the 5G network may be advantageous, they are vulnerable to security and have a disadvantage in that they are significantly larger than the 4G network. For example, when an unmanned vehicle using a 5G network is hacked, it is directly connected to a traffic accident, and hacked appliances are exposed to a risk of failure.

This report describes the features and technologies of the 5G network and the resulting weaknesses or security weaknesses. In addition, as a countermeasure against security weaknesses, introduction of quantum cryptography communication technology and standardization of 5G security will be introduced to find out what methods are being introduced and which methods are needed to enhance the security of the 5G network. DoS and DDoS attacks from vulnerable, large-scale connected devices can be a direct threat to 5G networks. According to the European ENISA Threat Landscape Report 2018 report, DDoS attack capacity continues to grow, DDoS attacks via IoT botnets appeared in 2016, and 1 terabyte DDoS attacks per GitHub (1.35 Tbps) in 2018. Since the attack, the magnitude of the attack has gradually increased to a maximum of 1.7 tera class.

2. 5G network

2.1 5G NR(New Radio)

Table 1. Comparison between 4G, 5G

Item	4G	5G
Peak data rate	1Gbps	20Gbps
User experienced data rate	10Mbps	100Mbps
Spectrum capacity	-	x3
Area traffic capacity	0.1Mbps/m^2	10Mbps/m^2
Latency	10ms	1ms
Connection density	100,000/km^2	1,000,000/km^2
Network energy efficiency	-	x100
Mobility	350km/h	500km/h

5G is a network technology that dramatically reduces delay time and speeds up to 10 times faster than 4G. In addition, the number of devices that can be connected per unit area is greatly increased, making computing much more effective than 4G [1]. Table 1 compares the performance of 4G and 5G.

5G NR means 5G mobile communication standard, and standardization is to enable mutual exchange or substitution between products. In addition to 5G NR, 5G security standards are underway in 3GPP and others. 5G uses network slicing technology that divides the network and transmits it according to the user, which enables faster transmission / reception. However, as data is processed at the base station to implement the network slicing technique, the risk of external attack also increases.

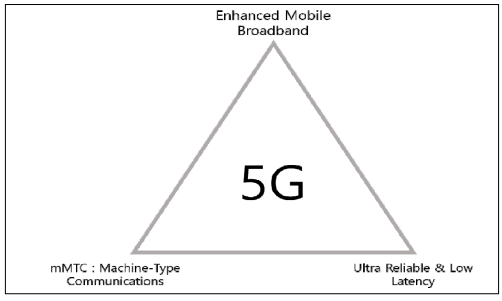


Fig. 1. 5G Network's feature

Fig. 1 shows the development goal of the 5G network. Clockwise from above

1. Ultra-wideband service
2. High reliability / Ultra low delay communication
3. Bulk connections

2.2 Network Slicing

Network slicing differs from shared networks that used up to existing 4G networks. As shown in [Fig 2], the shared network used up to 4G was a structure that directly accesses the network that each entity needs in the shared network. With the network slicing used in the 5G network, one physical network is divided into a plurality of virtual networks, and a virtual network is provided by containing only necessary networks for each entity. At this time, the network is separated in parallel.

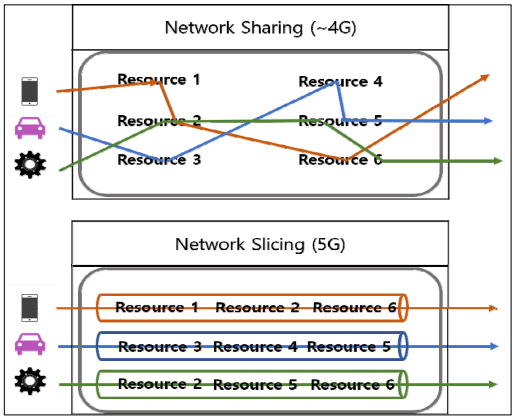


Fig. 2. Network Sharing, Network Slicing

Namely, it is possible to maintain quality without affecting other services through network slicing. In addition, since resources are allocated independently to the network, the time delay is drastically reduced [2,3].

First, in the standardization stage, communication protocols and interfaces must be securely designed for inter-working of networks and systems between countries. Until now, 3GPP standard has developed security standards for authentication and key management for mutual authentication between user and network, security standards to protect signaling message of control plane and data of user plane. Has been continually strengthened, but vulnerabilities in standard protocols may exist because the standard defines at least basic security requirements and specifications.

3. 5G security weakness, vulnerability

3.1 Base Station Data Processing

In case of existing 4G network, delay time is longer than 5G because it has to go through central server. In 5G, however, the edge computing function is introduced, and data is processed by placing the server close to the user. Here, the user is close to the base station, which means that the base station does not merely perform the role of an intermediary, but rather the server itself and processes the data.

If the number of servers increases, the number of hacking attempts increases naturally. In the case of existing 4G, if the path for data hacking was only the central server, data could easily be taken out even if only the base station is hacked in the 5G network.

In addition, since 5G is not fully established yet, a non-stand-alone 5G network that processes data with a 4G network is applied, and research has succeeded in sending texts against false disaster by hacking 4G LTE data network. Data security methods are essential [4].

3.2 DDoS risk due to the connection

The 5G network has a high-speed connection function. A super high-speed connection is a technique of greatly increasing the number of devices connectable per unit area, and more than one million devices can be connected per square kilometer. Through this, the 5G network can secure a lot of objects such as automobiles as well as connected smart phones and computers. This can also be a major weakness in security. When a hacker attacks a base station after hacking a plurality of devices within a unit area, it is a DDoS attack in itself, and it is also possible to attack the central equipment and cause a service failure.

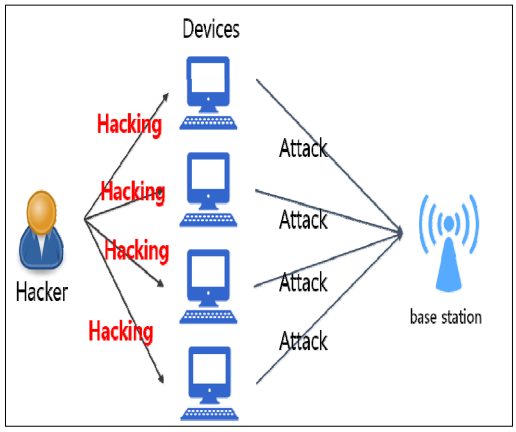


Fig. 3. Hacking

[Fig 3] shows the base station attack after hacking multiple devices. In this case, the base station may cause a service failure due to depletion of resources due to simultaneous attacks, and it is also possible to take data in response to a hacker's attempt.

3.3 Network Slice

The network slice is also positive in that it provides a dedicated network by allocating a virtual network, but there are matters to be considered in terms of security. The security considerations for the network slice were selected from ETRI's "Hyperlinked Intelligent Infrastructure Security Technology Trend - Mobile Security Center of 5G Era" [5].

1. Denial of service for other slices
2. Depletion of security resources on other slices
3. Sub-channel attack across the slice
4. Most attacks on network slice instances within the operator network
5. Impersonation attack on other network slice managers in the operator network
6. When the terminal is connected to multiple slices,

Also, there is a problem that the optimization of network slice is insufficient since standardization is still in progress. Since security is not properly equipped, there is a possibility that there are more security risks than the above six cases.

4. Solution

4.1 Quantum cryptography communication

Quantum Cryptography is an encryption technique using Quantum. According to ETRI's "Quantum Cryptography Communication Technology", quantum cryptography communication technology is based on the principle of quantum mechanics, so that it can not be eavesdropped or intercepted, thus ensuring absolute safety [6].

In Korea, SK Telecom acquired the quantum cryptographic communication company for the first time in the world and tried to compensate for the 5G security vulnerability.

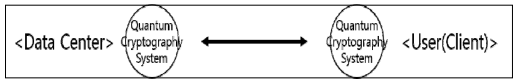


Fig. 4. Quantum Cryptography

[Fig. 4] shows quantum cryptography communication. The data center and the user each communicate using a quantum cryptographic communication system, where the sending and receiving sides have the same random bit string (password). Quantum technology is applied to the process of exchanging information for bit stream generation.

Another advantage of quantum cryptography is that it detects when an attempt is made to intercept or hack during cryptographic distribution. For eavesdropping, the quantum state transmission channel must be accessed and measured, but the quantum state transmitted due to the characteristics of both must be undermined. This will cause a random bit string to have a Quantum Bit Error Rate (QBER) error and reset the final secret key [7].

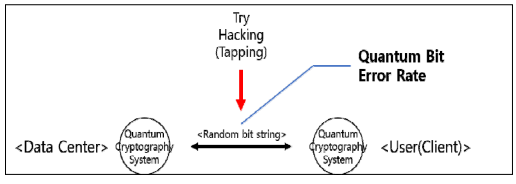
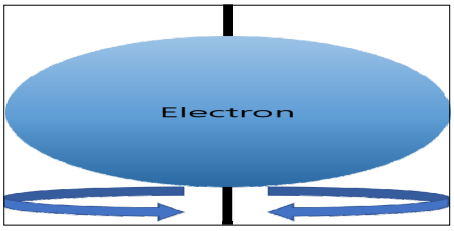


Fig. 5. QBER

[Fig. 5] shows the QBER generation process.

In quantum key distribution process, the phenomenon of quantum superposition is used. In quantum key distribution process, a quantum bit is used as a tool of information transmission. In other words, it means that there is not only one information in one quantum but also many duplicate quantum in one quantum. Because of this quantum superposition, a hacker can not

distinguish what information contained in both of them, even if they are duplicated, so the security is even better.



Fig,. 6. Quantum Superposition

[Fig 6] is related to quantum superposition. The electrons rotate around the axis, and different rotational states of electrons can exist at the same time. This is called quantum superposition.

In quantum cryptography, the photon used can be divided into a single photon and a multiphoton. Usually quantum cryptography uses a single photon because the risk of eavesdropping due to a PNS attack exists when using multiple photons.

4.2 5G Security Standardization

So far, if security was added to the existing structure, the method using 5G security standardization will consider security from the design stage [16].

5G, like the network slicing technology already described above, organic interaction is a key technology. In order to enable organic interactions, the need for standards is increased. At this time, it is important to consider not only design but also security technology, privacy, etc. [8].

In addition, the importance of 5G security standardization is that it is possible to systematically protect against hacking by building a versatile and robust security system. Currently, several organizations are working on 5G network standardization and 5G security standardization.

4.2.1 5G Security Standardization Status

Currently, many organizations including 3GPP are considering and studying security related standards, and there are four representative ones

1. 3GPP: Non-Standalone NR is defined as the first step of standardization for 5G coverage completion.
2. ITU: Six security standard roadmaps are established and standards development is being done.
3. NGMN
4. 5G PPP: 5G security threats and security structure are under study [9-16].

Part 1 : ICT Standards Development Organizations and Their Work
Part 2 : Approved ICT Security Standards
Part 3 : Security standards under development
Part 4 : Future needs and proposed new security standards
Part 5 : Best practices
Part 6 : IdM Landscape : IdM standards, organizations and gap analysis

Fig. 7. ITU 6 Road Maps

5. Conclusion

5G network, based on the core concepts of organistic and interaction unlike existing 4G, achieved dramatic speed improvement and delay time reduction compared to existing 4G. However, there is also a possibility that the technologies introduced for speed improvement may act as a security threat. Network slicing, edge computing, and high-end connectivity. A hacking method using this technique includes a method of attacking a base station by hacking a plurality of devices connected at a high rate, and a method of taking data processed by a base station using the loopholes of edge computing. Currently, 5G security standardization method is continuously discussed with introduction of quantum cryptography communication technology for 5G

security enhancement. Users can also protect against 5G network security threats by installing complementary tools such as vaccines on each device.

REFERENCES

[1] A. Petosa. (2018). Engineering the 5G Environment. 2018 IEEE 5G World Forum (5GWF).
DOI :10.1109/5gwf.2018.8516930

[2] E. Dahlman, S. Parkvall & J. Sköld. (2018). 5G Standardization. 5G NR: The Next Generation Wireless Access Technology, 7-25.
DOI :10.1016/b978-0-12-814323-0.00002-8

[3] T. Yoo. (2016). Network slicing architecture for 5G network. 2016 International Conference on Information and Communication Technology Convergence (ICTC).
DOI :10.1109/ictc.2016.7763354

[4] T. Wolf. (n.d.). Kr (Krypton). Ac - Na Landolt-Börnstein - Group III Condensed Matter, 352-352.
DOI:10.1007/10332996_91

[5] 5G Network Planning and Optimization. (2019). 5G Explained, 255-269.
DOI:10.1002/9781119275695.ch9

[6] D. J. Bernstein. (n.d.). Introduction to post-quantum cryptography. Post-Quantum Cryptography, 1-14.
DOI :10.1007/978-3-540-88702-7_1

[7] P. Kok & B. W. Lovett. (n.d.). Quantum communication with continuous variables. Introduction to Optical Quantum Information Processing, 255-293.
DOI : 10.1017/cbo9781139193658.009

[8] J. Lee & Y. Kwak. (2016). 5G Standard Development: Technology and Roadmap. Signal Processing for 5G, 561-576.
DOI :10.1002/9781119116493.ch23

[9] 5G Technology Revolution. (2017). International Journal of Modern Trends in Engineering & Research, 4(12), 135-140.
DOI:10.21884/ijmter.2017.4394.2tmix

[10] K. Asatani. (2018). Trends and Issues in 5G Networking and Beyond. *Journal of ICT Standardization, 5(3),* 203-224.
DOI : 10.13052/jicts2245-800x.531

[11] S. Hong, (2014). Research on Wireless Sensor Networks Security Attack and Countermeasures : Survey. *Convergence Society for SMB, 4(4),* 1-6

[12] E. Choi. (2018). Visualization Management Convergence Access Control Model for Cloud Environments. *Journal of Convergence for Information Technology, 8(5),* 69-75

[13] D. Yeom. (2018). Remote Control of Network-based Modular Robot. *Journal of Convergence for Information Technology, 8(5),* 77-83

[14] Y. Jeong. (2018). User Privacy Management Model using Multiple Group Factor based on Blockchain. *Journal of Convergence for Information Technology, 8(5),* 107-113
DOI : 10.22156/CS4SMB.2018.8.5.107

[15] K. I. Kim, (2018). Differences Between Client's and Supplier's receptions of IT Outsourcing Risks. *Journal of Convergence for Information Technology, 8(5),* 237-242.
DOI : 10.22156/CS4SMB.2018.8.5.237

[16] S. Anamalamudi, A. R. Sangi, M. Alkatheiri, F. T. B. Muhaya & C. Liu. (2018). 5G-WLAN Security. A Comprehensive Guide to 5G Security, 143-163.
DOI : 10.1002/9781119293071.ch7

홍 성 혁(Sunghyuck Hong) **[정회원]**

- 2007년 8월 : Texas Tech University, Computer Science (공학박사)
- 2012년 3월 ~ 현재 : 백석대학교 정보통신학부 부교수
- 관심분야 : 블록체인, 사물인터넷 보안, 경량보안프로토콜
- E-Mail : shong@bu.ac.kr