engineering proceedings

MDPI

Proceeding Paper

Cyber Security in a 5G-Based Smart Healthcare Network: A Base Station Case Study †

Meng-Huan Lee, I-Hsien Liu, Hsiao-Ching Huang and Jung-Shian Li *

Department of Electrical Engineering, Institute of Computer and Communication Engineering, National Cheng Kung University, Tainan 70101, Taiwan; mhlee@cans.ee.ncku.edu.tw (M.-H.L.); ihliu@cans.ee.ncku.edu.tw (I.-H.L.); hchuang@cans.ee.ncku.edu.tw (H.-C.H.)

* Correspondence: jsli@cans.ee.ncku.edu.tw

† Presented at the IEEE 5th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability, Tainan, Taiwan, 2–4 June 2023.

Abstract: 5G is transforming the healthcare industry by providing novel use cases and applications. With a lower latency, a higher bandwidth, and massive machine-type communication capabilities, 5G supports the smart healthcare system in expanding its applications. This rapid adoption of 5G technology increased the number of connected devices. However, the deployment of 5G networks also introduced security challenges, especially for sensitive patient data which must be secured. Base stations are a key component in connecting devices to the mobile network and need to be secured. As unauthorized base stations cause interference or can be used as fake base stations to attack devices in the network, it is crucial to address the security concerns associated with 5G-based smart healthcare networks. Thus, we studied the case of base station security to investigate different methods for detecting and mitigating the risks associated with unauthorized base stations. The results can be used to better secure 5G-based smart healthcare networks.

Keywords: 5G; smart healthcare; base station; cyber security

check for updates

Citation: Lee, M.-H.; Liu, I.-H.; Huang, H.-C.; Li, J.-S. Cyber Security in a 5G-Based Smart Healthcare Network: A Base Station Case Study. *Eng. Proc.* **2023**, *55*, 50. https://doi.org/10.3390/engproc2023055050

Academic Editors: Teen-Hang Meen, Kuei-Shu Hsu and Cheng-Fu Yang

Published: 5 December 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Amid the COVID-19 pandemic, the use and demand for telemedicine and remote healthcare have increased significantly. Thus, new approaches for smart healthcare are required for urgent application [1]. Smart healthcare integrates advanced technologies such as 5G, Internet of Things (IoT) devices, AI, and data analytics into the healthcare industry. It revolutionizes the delivery of healthcare services by enabling real-time monitoring, personalized treatment, and improved patient outcomes. Interconnected devices and networks are used to collect and analyze health data, facilitating remote monitoring, telemedicine consultations, and efficient data management. Wearable devices are used to monitor vital signs for early detection and personalized interventions [2]. Smart healthcare systems empower patients and provide access to medical records, personalized recommendations, and virtual consultations. They also optimize care resource utilization and enhance the efficiency of healthcare delivery.

Figure 1 illustrates an example architecture of a 5G-based smart healthcare network connecting different devices to healthcare services. With the help of 5G, these applications have become more reliable than before while serving more people in rural areas where healthcare services were not easily available. The rapid adoption of 5G and IoT technology increases the number of connected devices, including medical devices such as blood glucose meters and heart rate monitors. These devices collect sensitive patient data that must be protected from cyber-attacks. Base stations, which act as access points between these devices and the network, are particularly vulnerable to cyber-attacks, as they are exposed to public internet or radio attacks. Therefore, addressing cyber security concerns in 5G-based smart healthcare networks is of paramount importance. Therefore, we explored base

station security and how fake base stations became a threat to a smart healthcare network. Then, possible measures were proposed to secure and detect such threats.

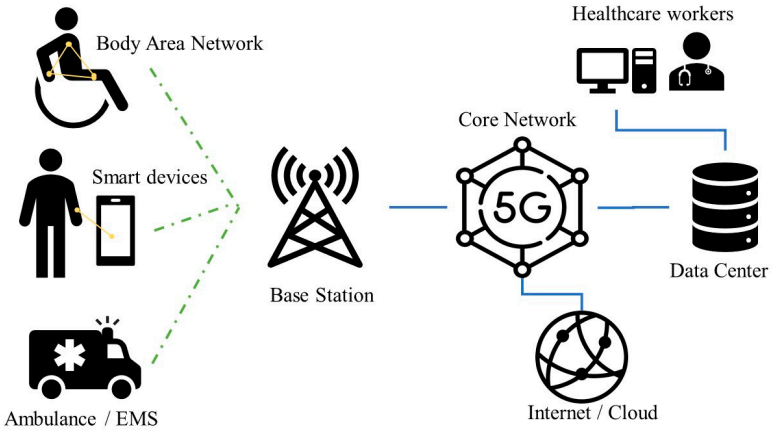


Figure 1. Example of a 5G-based smart healthcare network.

2. Research Background

We reviewed the related studies on 5G and 5G-based smart healthcare networks to define cyber security problems in their use.

2.1. 5G and 5G-Based Smart Healthcare Networks

5G is an advanced mobile network technology that provides a low latency, a high bandwidth, and massive machine-type communications serving large numbers of IoT applications. These applications range from cars and robots to sensors and, in the context of smart healthcare, medical equipment and wearable electronics. A 5G network mainly comprises user equipment (UE), base stations, and core network [3], as follows:

- The UE is a modem and stores a permanent identifier called International Mobile Subscriber Identity (IMSI) and a key used for mutual authentication between the user and the network.
- The base station (BS) acts as the access point for UEs to attach to the Radio Access Network (RAN), connecting it to the mobile network and, thus, to the Internet.
- The core network (CN) is the backbone of the mobile network; it performs all management tasks and traffic routing.

Reference [4] described the architecture of 5G and IoT-enabled smart healthcare considering specific key-enabling technologies such as small cells and the software-defined network (SDN). A taxonomy for 5G smart healthcare was also explained, and future research opportunities applied to IoT-based 5G smart healthcare were reviewed. In Taiwan, a 5G-based smart healthcare network has been trialed in hospitals with mobile network operators that deployed 5G private networks. In the network, medical robots were used to help doctors and nurses [5].

2.2. Cyber Security in a Smart Healthcare Network

The cyber security of a smart healthcare network is important in safely deploying its healthcare services. Securing sensitive data and personal smart healthcare devices is critical to the protection of the privacy of patients and medical personnel. A smart healthcare service is also a mission-critical application that involves human well-being, which requires high availability and reliability. Any security breach or service interruption threatens patients and working personnel. Ahad et al. presented a comprehensive review of 5G-based smart healthcare network security [6]. They investigated various technological features and services related to 5G smart healthcare security, including authentication, confidentiality availability, non-repudiation, and integrity. They also discussed many security threats in 5G smart healthcare and proposed available solutions for issues of 5G-

based smart healthcare security. Algarni classified schemes for smart healthcare systems to explore important security issues and challenges and propose countermeasures and directions for future research [7].

3. Base Station Security

Base stations play an important role in a mobile network and are terminals for encryption and integrity protection. Therefore, they are accessible to anyone controlling them and implementing the software. We reviewed the security issues involved in the RAN and BSs.

3.1. Security of Base Station in a Mobile Network

The security of a BS and RAN is often underestimated in a mobile network compared to the UE and CN. Securing the BS helps protect the mobile network as a whole. From the perspective of security, the BS acts as the first line of defense against unauthorized access and malicious activities by enforcing authentication and encryption protocols, monitoring network traffic, and detecting and mitigating potential threats. For 5G to facilitate a higher demand and amount of devices, the number of base stations is much larger than in previous generations. A large number of base stations are now processing large amounts of data.

3.2. Fake Base Station

A fake base station (FBS), also known as a rogue base station (RBS), is a type of malicious device that impersonates a real base station. The main goal of the attacker is to trick UEs into connecting to unauthorized services and/or to steal the identity of the user by tracking and collecting IMSI information from the user's devices [8]. These "IMSI-Catchers" have been spotted since the use of 2G globally. There are reports of suspicious devices appearing in major cities and records of law enforcement using similar equipment to conduct surveillance on suspects [9–11]. There was a recent case of using a fake BS for phishing in Taiwan. The suspects were found to have purchased the fake BS in China to transmit phishing SMS messages to trick people into giving away their credit card information. For this, they downgraded the victims' smartphones to use 2G networks, so the victims were disconnected from the legitimate 4G/5G BS and became vulnerable to phishing messages [12]. Similar cases had been also found in China before and characterized to provide insights into the FBS spam ecosystem in China [13]. A typical procedure for using a fake BS is illustrated in Figure 2.

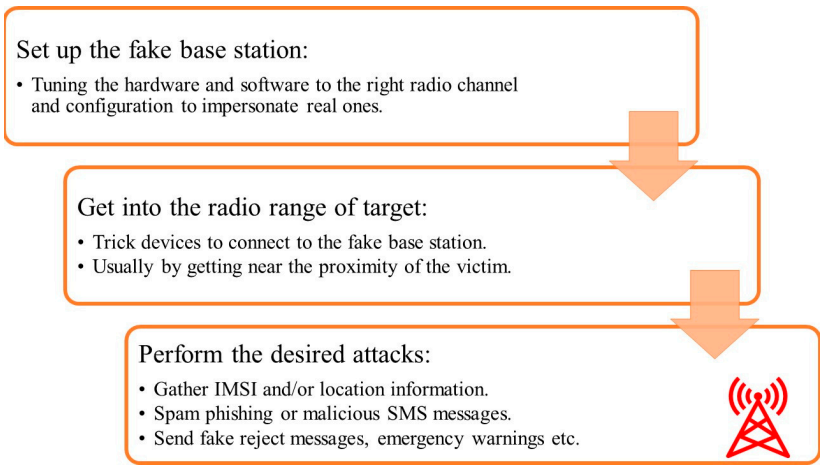


Figure 2. Typical procedure of cyber-attacks using an FBS.

In using FBSs for phishing to steal credit card information in a 4G/5G mobile network, phishing messages are usually modified to cheat unsuspected victims with fake hospitals, healthcare websites, or banks. For example, during the pandemic, a fake website of an economic relief package application was spread on social media. Advanced fake BSs are

capable of performing Denial-of-Services (DoS) and Man-in-the-Middle (MitM) attacks. While the cost of deploying mobile networks becomes cheaper thanks to much research and development, so does the cost for malicious cyber-attacks to obtain the hardware and software for setting up FBSs. Thus, cyber-attacks using low-cost FBSs are increasing (Figure 3).

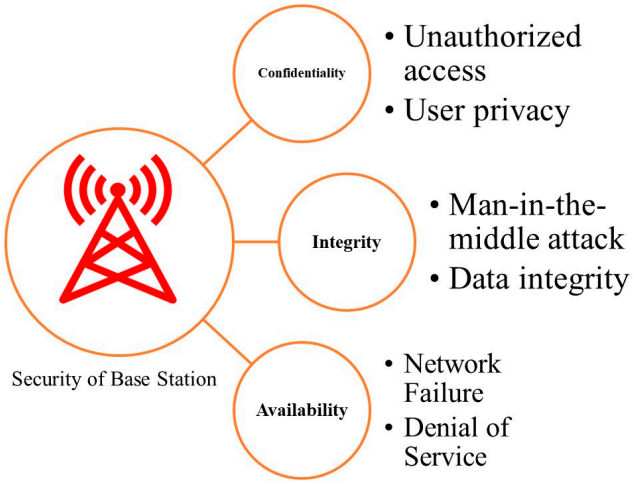


Figure 3. Security threat of a base station.

3.3. Threat to a Smart Healthcare Network

FBSs are a threat to smart healthcare networks. These threats were described in terms of confidentiality, integrity, and availability in a CIA triad model, as follows:

- Confidentiality: Malfunctioned access control and authentication allow unauthorized access to a BS, leading to malicious cyber-attacks on sensitive healthcare data. Poorly implemented encryption makes system information and user data vulnerable to cyber-attacks. As a result, patients' privacy is infringed by the theft of sensitive healthcare data.
- Integrity: An FBS is placed between the victims and the real BS and is open to MitM attacks. Information transmitted between the devices and the base station is intercepted and modified to steal smart healthcare data.
- Availability: An FBS causes a DoS, and sensors and devices in the healthcare network lose their connections to the real network, which paralyzes healthcare services and data.

4. Discussion

Potential solutions for security problems are necessary to protect base stations in 5G-based smart healthcare networks. The following needs to be considered for networks' security in this study.

Solution for Security

To prevent sensitive data from being exposed to a public mobile network, the use of a private network dedicated to smart healthcare is encouraged. In a private network of institutions, their connectivity can be more easily controlled, and the specific needs of a smart healthcare service also can be satisfied. The private network still is vulnerable to cyber-attacks using an FBS on the wireless interface. Several private networks share resources with public networks through network function virtualization (NFV). In this case, if the shared BS is attacked, the private network service is also affected [8]. Cryptography and blockchain technology can be used to protect the network. Novel approaches were already proposed for using those methods. Blockchain technology stores records and allows safe and transparent data sharing for patients and network users. The decentralized

framework provided by the distributed ledger facilitates privacy needs for numerous applications in 5G. However, blockchain requires considerable computing power for small IoT devices [14]. Detecting suspicious BSs for potential threats is necessary to identify threats and take action before the damage occurs. To detect an FBS, network-, signal-, and location-based detection schemes were suggested for 5G smart healthcare networks [15,16].

5. Conclusions

We explored the cyber security of 5G-based smart healthcare networks with an emphasis on BSs. We reviewed the related literature to explore the increasing importance of the rapid expansion and importance of cyber security for 5G smart healthcare networks and the IoT devices connected to them. Through a detailed investigation of the FBS attacks in Taiwan, the security problems caused by FBSs were analyzed to describe the failure to secure BSs and 5G-based smart healthcare networks. Potential security measures and technology were also proposed to raise awareness of the importance of cyber security in 5G smart healthcare networks.

Smart healthcare and mobile network technology are constantly evolving, and so are cyber-attackers. Although the proposed solutions are considered to solve security problems, it is still necessary for healthcare service providers to be alerted to an increasing number of exploits and attacks. Developing safe and efficient authentication methods is key for the security of smart healthcare networks and connected devices. However, networks and devices have different computing powers. Therefore, an ideal algorithm is required for security by minimizing latency and computing costs. The large amounts of sensitive data on the network require improved privacy and proper encrypted and processed methods. Policies and security standards must be updated often to keep up with the constantly evolving security threats. Healthcare workers, patients, and administrators must be aware of the threats to smart healthcare technology.

Author Contributions: Validation, H.-C.H.; Writing—original draft, M.-H.L.; Writing—review & editing, I.-H.L.; Supervision, J.-S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract numbers 111-2221-E-006-079- and 112-2634-F-006-001-MBK.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data available on request due to restrictions e.g., privacy or ethical. The data presented in this study are available on request from the corresponding author. The data are not publicly available due to the dataset containing base station signal records that do not comply with regulatory approvals.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Taiwo, O.; Ezugwu, A.E. Smart healthcare support for remote patient monitoring during COVID-19 quarantine. *Inform. Med. Unlocked* **2020**, *20*, 100428. [CrossRef] [PubMed]
2. Baker, S.B.; Xiang, W.; Atkinson, I. Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities. *IEEE Access* **2017**, *5*, 26521–26544. [CrossRef]
3. 3GPP TS 23.501 System Architecture for the 5G System (5GS). Available online: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf (accessed on 22 April 2023).
4. Ahad, A.; Tahir, M.; Yau, K.-L.A. 5G-Based Smart Healthcare Network: Architecture, Taxonomy, Challenges and Future Research Directions. *IEEE Access* **2019**, *7*, 100747–100762. [CrossRef]
5. Taipei City Government. 5G Private Network Intelligent Disinfection and Transportation Robot. Available online: https://smartcity.taipei/projdetail/175?lang=en (accessed on 12 May 2023).
6. Ahad, A.; Ali, Z.; Mateen, A.; Tahir, M.; Hannan, A.; Garcia, N.M.; Pires, I.M. A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions. *Array* **2023**, *18*, 100290. [CrossRef]

7. Algarni, A. A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. *IEEE Access* **2019**, *7*, 101879–101894. [CrossRef]
8. Lee, M.-H.; Liu, I.-H.; Li, J.-S. Fake Base Station Threats in 5G Non-Public Networks. In Proceedings of the ICAROB 2023, Oita, Japan, 9–12 February 2023.
9. Cullen, C.; Bureau, B. Someone Is Spying on Cellphones in the Nation's Capital. CBC News. Available online: https://www.cbc.ca/news/politics/imsi-cellphones-spying-ottawa-1.4050049 (accessed on 7 March 2023).
10. Ramirez, A. *ICE Records Confirm That Immigration Enforcement Agencies Are Using Invasive Cell Phone Surveillance Devices*; American Civil Liberties Union: New York, NY, USA, 2020.
11. Chlosta, M.; Rupprecht, D.; Pöpper, C.; Holz, T. 5G SUCI-catchers: Still catching them all? In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), New York, NY, USA, 28 June–2 July 2021.
12. Chiang, Y.; Su, S.; Ko, L. 12 Indicted over Credit Card Fraud Using Fake Base Stations. Focus Taiwan. Available online: https://fostaiwan.tw/society/202304100016 (accessed on 22 April 2023).
13. Zhang, Y.; Liu, B.; Lu, C.; Li, Z.; Duan, H.; Hao, S.; Liu, M.; Liu, Y.; Wang, D.; Li, Q. Lies in the Air: Characterizing Fake-base-station Spam Ecosystem in China. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). Association for Computing Machinery, New York, NY, USA, 9–13 November 2020; pp. 521–534.
14. Tahir, M.; Habaebi, M.H.; Dabbagh, M.; Mughees, A.; Ahad, A.; Ahmed, K.I. A review on application of blockchain in 5G and beyond networks: Taxonomy, field-trials, challenges and opportunities. *IEEE Access* **2020**, *8*, 115876–115904. [CrossRef]
15. Park, S.; Shaik, A.; Borgaonkar, R.; Martin, A.; Seifert, J.P. White-Stingray: Evaluating IMSI Catchers Detection Applications. In Proceedings of the Workshop on Offensive Technologies (WOOT), Vancouver, BC, Canada, 14–15 August 2017.
16. Huang, K.-W.; Wang, H.-M. Identifying the Fake Base Station: A Location Based Approach. *IEEE Commun. Lett.* **2018**, *22*, 1604–1607. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.