Security of Mobile Wireless Networks

Ryan Shah
Kennesaw State University
IT4833: Wireless Security
Professor Seyedamin Pouriyeh
July 23, 2023

Introduction

As wireless technology continues to evolve the security of our networks becomes increasingly important. With the rise of 4G, 5G, and even 6G networks now we are able to connect to the internet at faster speeds and with greater reliability than ever before. However, these advancements also bring new security challenges that must be addressed to protect our personal/sensitive information. In this report, we will explore the security threats facing 4G, 5G, and 6G wireless networks and the measures that can be taken to mitigate these risks.

4G Security

With 4G still being around in modern-day society and mobile devices growing at an exponential rate it is still important to highlight the security of 4G. According to Statistica, in 2021 there were nearly 15 billion mobile devices in use globally and in 2025 it is projected that there will be 18.22 billion mobile devices in use worldwide. This shows the growth of mobile devices worldwide and why we need to talk about the security of these different cellular networks. Like all technologies, 4G networks are susceptible to various security threats. These include attacks targeting mobile devices/infrastructure, the exploitation of newly connected devices, and the repurposing of old Internet techniques to exploit broadband data services. Several measures can be taken to mitigate these threats. One crucial step is to provide people with education on the best security practices/proper data handling. Enforcing robust password policies and limiting access to sensitive data can also help reduce the risk of security breaches. Also, regularly backing up data can help prevent data loss in the event of a breach.

Some issues mentioned in the research paper were physical layer issues such as interference and scrambling attacks. Interference attacks on 4G networks are relatively simple to execute due to the widespread availability of the necessary equipment and knowledge. However, the research shows that these attacks can be easily detected using radio spectrum monitoring tools. By employing radio-direction-finding tools the source of interference can be located. Additionally, increasing the strength of the source signal and utilizing spreading techniques can enhance its resistance to interference. Although interference is a significant concern, its impact on 4G networks and users is likely to be minimal due to the ease of detection and mitigation. Scrambling is a type of interference that occurs for brief periods and targets specific frames or portions of frames. An attacker may aim to disrupt service by targeting the management or control information of a particular user. However, successfully executing a scrambling attack requires a high level of sophistication and knowledge, as the attacker must identify the specific frames and time slots to target. As such, scrambling is challenging to carry out effectively (Seddigh et al., 2010).

5G Security

The 5G network has expanded drastically over the past couple of years with the newer model phones being named “5G devices” it is important to highlight the security of this cellular network. The second research paper discusses security attacks used in 5G including eavesdropping, traffic analysis, DoD/DDoS, and MITM. Eavesdropping is a type of passive attack where an unauthorized person intercepts a message between others. Since it doesn’t affect normal communication it’s difficult to detect. To prevent eavesdropping signals are often encrypted over the radio link making it impossible for the eavesdropper to directly intercept the received signal. The effectiveness of encryption in preventing eavesdropping depends on the strength of the encryption algorithm and the computing power of the eavesdropper. With the rapid advancement of computing power/data analysis technologies eavesdroppers can use these

new technologies to their advantage. Existing mechanisms to combat eavesdropping face challenges as many assume a small number of applied improvements to detection for better error rate performance. Traffic analysis is a passive attack where an unauthorized person intercepts information such as the location and identity of communicating parties by analyzing the traffic of the received signal, without understanding its content. Even if the signal is encrypted, traffic analysis can reveal patterns of communication. This type of attack doesn't affect legitimate communications. DoS attacks can overwhelm network resources making them unavailable to users. These attacks can be launched using jamming techniques and can occur at different layers of the network. When multiple adversaries are involved, the attack becomes a Distributed Denial of Service (DDoS) attack. Detection is currently the primary method for identifying these attacks. With the increasing number of devices connected to 5G wireless networks, DoS and DDoS attacks pose a significant threat to network operators. These attacks can target either the network infrastructure or individual devices and users, affecting various components such as signaling, user and management planes, support systems, radio resources, and physical/logical resources. A DoS attack against a device or user can target components such as battery, memory, disk, CPU, radio, and sensors. A Man-in-the-Middle (MITM) attack occurs when an attacker secretly intercepts and alters the communication between two legitimate parties. This type of attack can happen at different layers of the network and aims to compromise the confidentiality, integrity, and availability of the data being transmitted. One proposed method for detecting both random and malicious errors in 5G networks is the use of Cyclic Redundancy Check (CRC) based message authentication, which can help detect these attacks without increasing bandwidth usage (Fang et al., 2017).

The third research paper explains the security challenges in 5G-enabled vehicular networks which I thought interesting. One of the new application scenarios in 5G vehicular networks is cooperative driving which enables autonomous vehicles to drive in a platoon formation to reduce fuel consumption and minimize the risks associated with human error. However, this service is vulnerable to Sybil attacks where an attacker creates multiple fake identities and message falsification, which can compromise the safety of V2V communication and potentially cause serious traffic accidents. Cyberattacks are a significant threat to the vehicle industry. While there has not yet been a major malicious cyberattack on a vehicle the potential for danger does exist. Hackers have demonstrated the ability to remotely access and control a vehicle's systems, including the accelerator and brakes. In the future, it is possible that hackers could develop viruses that could spread from vehicle to vehicle, posing a significant threat to 5G-enabled vehicles (Lai et al., 2020).

6G Security

The 6G network is the latest installment coming to cellular in the coming years. It is still in early development. The White House has started planning for the development of 6G technology. They intend to meet with government officials and business leaders to discuss how to build the next generation of 6G wireless technology using lessons learned from the deployment of 5G. The administration believes that by integrating elements such as AI, advanced software, and cloud computing they can create faster networks that can support applications in various fields such as health, energy, transportation, water, and agriculture. In addition, a research team at the City University of Hong Kong has developed an innovative tunable terahertz (THz) meta-device that can control the direction and coverage area of THz beams. By rotating its meta surface the device can quickly direct the 6G signal to a specific

recipient reducing power leakage and increasing privacy. This is expected to provide a highly adjustable, directional, and secure means for future 6G communication systems.

The last research paper talks about 6G security challenges and potential solutions. With the introduction of Further enhanced Mobile Broadband (FeMBB), the processing of high data rates for security purposes, such as attack detection, AI/ML pipelines, traffic analysis, and pervasive encryption, will pose challenges. Distributed security solutions can help alleviate this issue by processing traffic locally and on-the-fly in different segments of the network from the edge to the core service cloud. Distributed Ledger Technology (DLT) will play a key role in providing transparency, security, and redundancy. Ultra massive Machine Type Communication (umMTC) will support critical use cases that require much stricter security measures than 5G. The Internet of Everything (IoE), with its diverse capabilities, will present challenges for the deployment and operation of security solutions such as distributed AI/ML and privacy concerns. A crucial aspect is how to integrate new security enablers into a large number of resource-constrained devices. However, enforcing security will become more complex as network entities become more mobile and change their edge network. Advancements in circuits, antennas, meta-material-based structures, and AI chips have paved the way for a paradigm shift in hardware. This can lead to faster feedback, reduced latency, lower costs, and improved operation. Also, since Edge Intelligence (EI) gathers data from multiple sources and the results of AI/ML algorithms are highly dependent on data EI is vulnerable to various security attacks. Attackers can exploit this dependency to launch attacks such as data poisoning/evasion or privacy violations which can affect the outputs of AI/ML applications and undermine the benefits of EI. The wide range of 6G requirements and the envisioned full end-to-end (E2E) automation of network and service management using AI demand a significant change in network service orchestration and management in 6G architecture. The ETSI ZSM (Zero-touch network and Service Management) architecture for 5G is a promising initiative toward this intelligent network management deployment. However, several security challenges have been identified in such deployments. For example, closed-loop network automation may introduce security threats such as Denial of Service (DoS), deception, and Man-In-The-Middle (MITM) attacks. DoS attacks can be performed by gradually adding fake heavy loads to virtual network functions (VNFs) to increase the capacity of virtual machines (VMs). MITM attacks can be performed by triggering fake fault events and intercepting domain control messages to reroute traffic via malicious devices. Deception attacks can be performed by tampering with transmitted data. If 6G networks use Intent-Based Interfaces similar to ZSM, they can be vulnerable to information exposure, undesirable configuration, and abnormal behavior attacks. Intercepting information of intent by unauthorized entities can harm system security objectives such as privacy and confidentiality and lead to further subsequent attacks. Undesirable configurations in Intent-Based Interfaces, such as changing the mapping from intent to action or decreasing the security level, can jeopardize the security of the entire management system. A malformed intent could also have similar effects (Porambage et al., 2021).

Conclusion

In conclusion, the security of mobile wireless networks is a critical concern, especially with the increasing reliance on these networks for communication and data transfer. As technology advances and new generations of networks such as 4G, 5G, and 6G are introduced, new security challenges arise. While these networks offer faster speeds and improved performance, they also introduce new vulnerabilities that must be addressed to ensure the safety and privacy of users. It is essential for network providers and governments to work together to develop/implement robust security measures to protect against potential threats and ensure the continued growth/success of mobile wireless networks.

Works Cited

Fang, D., Quan, Y., & Hu, R. Q. (2017, December 4). Security for 5G Mobile Wireless Networks - IEEE Xplore. https://ieeexplore.ieee.org/document/8125684/

Lai, C., Lu, R., Zheng, D., & Shen, X. (2020, April 2). Security and privacy challenges in 5G enabled vehicular networks | IEEE https://ieeexplore.ieee.org/abstract/document/9055735/authors

Laricchia, F. (2023, March 10). *Number of mobile devices worldwide 2020-2025*. Statista. https://www.statista.com/statistics/245501/multiple-mobile-device-ownership-worldwide/

Porambage, P., Gür, G., Osorio, D. P. M., Livanage, M., & Ylianttila, M. (2021, July 28). 6G security challenges and potential solutions | IEEE conference . https://ieeexplore.ieee.org/abstract/document/9482609/

Seddigh, N., Nandy, B., Makkar, R., & Beaumont, J.-F. (2010, September 30). Security advances and challenges in 4G wireless networks | IEEE . https://ieeexplore.ieee.org/document/5593244/