PROTOCOLS USED IN 4G AND 5G NETWORKS AND ASSESSMENT OF THEIR SECURITY EFFECTIVENESS

Rakhmonov Ozodbek Shavkatjon ugli
Assistant teacher of TUIT Fergana branch

Abstract

This article evaluates the effectiveness of security measures used in 4G and 5G networks. It shows the vulnerability and resilience of 4G and 5G networks as a result of DDoS, Eavesdropping, Man-in-the-Middle, Signal Hijacking and Sim Cloning attacks. A brief overview of security vulnerabilities in 4G and 5G. Information about existing and possible problems in the 5G network is provided.

Keywords

DDoS, protocols, network security, network, cyber attacks, 4G, 5G, Eavesdropping, network monitoring.

Introdution

Along with the rapid development of mobile communication networks, the issues of information security are also increasing their relevance. 5G networks provide new opportunities and technologies, and it is necessary to ensure a high level of security during their use.

Although there are significant upgrades and changes in the 5G mobile communication network, there are still various levels of security issues. These challenges require the development of strong security and privacy policies in 5G networks and security protocols. At the same time, with the development of technology, security measures also require updating. Below are some of the challenges faced by 5G networks.

Expanded attack surface. 5G networks will support billions of devices. Including IoT (Internet of Things) devices. The large number of connections creates new opportunities for attackers, as each device or connection can become a potential security hole. IoT devices are particularly vulnerable to threats due to the lack of built-in security protections.

Integration problems with legacy networks. 5G networks are often used in conjunction with older 4G networks. This integration increases the risk of 4G security issues affecting 5G networks in the early stages. Despite updated security measures, when combined with older technologies, the risk of vulnerabilities increases.

Cyber attacks and network monitoring. 5G networks will handle massive amounts of traffic. This complicates real-time network monitoring and security. It has become difficult to accurately and quickly analyze traffic and detect cyber attacks.

Unknown vulnerabilities. Since 5G technology and some of the protocols used in it are new, there may be many unknown vulnerabilities and security issues. Attackers can exploit these vulnerabilities. This requires regular security updates in 5G networks.

Supply Chain Vulnerabilities. Many companies and suppliers are involved in building and maintaining 5G networks. Vulnerabilities in the supply chain, especially network access through network equipment or software vendors, can create additional opportunities for attackers.

Legal and Privacy Issues. Large amounts of data will be transmitted over 5G networks, and this will require increased protection of users' personal data. Globally, there are still no clear regulations on user data privacy and legal compliance, which creates challenges.

High risk of attacks. 5G networks will contain complex technologies and will serve IoT, automated systems and critical infrastructure. These services can be a target for cybercriminals. Attacks against 5G networks can seriously damage the operation of large systems (for example, transportation, energy, healthcare).

Network characteristics. Virtualization and cloud technologies are widely used in 5G networks, which creates new opportunities for cyber attacks on network infrastructure. Virtualization and cloud technologies require a high level of security because multiple users or services run simultaneously in a cloud environment.

Discussion

4G and 5G networks have similarities and differences. First, let's look at the general aspects.

- Encryption. In both networks, the data is encrypted using different encryption algorithms, which ensures the confidentiality of the data.

- Authentication: Users and devices are authenticated, allowing access to the network to be controlled.

- Absolute Control: Both networks have network control mechanisms that allow efficient network management and quick problem detection.

To assess the resilience of network security, we examine the resilience of DDoS attacks.

Now let's look at the different aspects of 4G and 5G networks.

The differences are mainly in new security approaches and improved technologies. 5G technology focuses more on security and aims to overcome some of the vulnerabilities found in 4G networks. Because as the speed increases, it becomes more difficult to protect the network.

SIR Publishers
CENTER FOR INTERNATIONAL
SCIENTIFIC PUBLICATIONS

JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN(Online): 2984-6722
SJIF Impact Factor |(2024): 6.752|
Volume-7, Issue-10, Published |20-10-2024|

The first difference is the level of encryption. While 4G networks use 128-bit encryption technology, which provides a high level of security, 5G networks have taken this protection even further and introduced 256-bit encryption. This is especially important in ensuring that data is protected from unauthorized access.

Another important difference can be seen in the identification and authentication processes. In 4G networks, the user identity (IMSI) is transmitted over the network in plain sight, increasing the risk of unauthorized access. 5G networks, on the other hand, use a technology called Subscriber Concealed Identity (SUCI) to transmit the IMSI in an encrypted state, which increases the level of security and helps to hide the user's identity.

Method

In order to evaluate the security of 4G and 5G networks, various experimental attacks are carried out on the networks and the tolerance percentages of the networks are determined based on the obtained results.

Research

We compare the results of experimental attacks on 4G and 5G mobile networks using data from various sources and experimental tests.

The 4G network has a centralized architecture, and when DDoS attacks occur on certain devices in the network, devices in the system may be affected. The tolerance level against DDoS attacks is estimated to be around 62-71%. That is, when 1000 DDoS attacks are carried out, 290-380 can damage the network.

Unlike 4G, the 5G network has a decentralized architecture, with different parts of the network operating independently. This architecture enables detection and isolation of attacks in a short period of time. This reduces the risk of DDoS attacks spreading across the network. Therefore, the tolerance level of 5G network is estimated to be improved to 84-90%. This means that out of 1000 DDoS attacks, only 100-160 can disrupt network activity.

Importance of security protocols in network security

The security protocols (IPSec and TLS) used to prevent DDoS attacks in 4G network can reduce the impact of attacks in some cases, but the ability to prevent these attacks is limited. The probability of this protocol reducing the network efficiency of DDoS attacks is 25-30% in the average case.

5G networks will use new protocols such as Network Slicing, Service-Based Architecture (SBA) and Enhanced Security Edge Protection Proxy (SEPP), and 4G networks will use updated and enhanced versions of existing protocols. These protocols increase the ability to detect and defend against DDoS attacks. As a result, the probability of DDoS attacks affecting network efficiency is estimated at 15-20%.

Additional protection mechanisms

In 4G networks, additional security measures are limited and mostly tied to the core network. This increases the probability of network stability degradation during DDoS attacks.

Network Function Virtualization (NFV) and Software-Defined Networking (SDN) technologies have been introduced in 5G networks, and these technologies provide an opportunity to flexibly change and protect network functions. Thanks to these technologies, the tolerance level of the network is improved by 40-50%.

In general, 5G networks are more resistant to DDoS attacks than 4G, thanks to new security protocols and the network's decentralized architecture.

Results

The results of DDoS, Eavesdropping, Man-in-the-Middle, Signal Hijacking and Sim Cloning attacks on 4G and 5G mobile networks will be presented with the help of a table.

Type of attack	4G (number of breaches per 1000 attacks)	4G attack tolerance percentage	5G (number of breaches per 1000 attacks)	5G attack tolerance percentage
DDoS	327	67.3%	162	83.8%
Eavesdropping	87	90.9%	12	99.0%
Man-in-the-Middle (MitM)	179	82.1%	80	92.0%
Signal Hijacking	288	71.2%	42	95.8%
Sim Cloning	213	78.7%	54	94.6%

Conclusion

While security measures were effective in 4G networks, 5G networks have significantly strengthened security protocols and architecture. Enhanced encryption, authentication processes, and user identification are more advanced in 5G networks than in 4G networks. Therefore, 5G networks are more compatible with modern security requirements and are distinguished by durable and robust protection measures against cyber attacks.

In order to fulfill security requirements, it is necessary to start creating a data protection system from the design and construction stage of mobile communication systems.

USED LITERATURE

1.   Madhusanka Liyanage, Ijoz Ahmed "A comprehensive guide to 5G security" John Wiley & Sons Ltd. - 2018.

2.   Amitava Ghosh, Rapeepat Ratasuk, Simone Redana, Peter Rost "5G-Enabled Industrial IoT Networks" Artech House - 2022y.

3.   Rakhmonov O. Sh., Musojonov H.M., Abdullayev A.R., "SECURITY PROTOCOLS, SAFEGUARDING THE DIGITAL FRONTIER", Scientific Journal "*SCHOLAR*" 1 (30): [70-74].

URL: https://researchedu.org/index.php/openscholar/article/view/5262

4.   Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila and A. Gurtov, "Overview of 5G Security Challenges and Solutions," in *IEEE Communications Standards Magazine*, vol. 2, no. 1, pp. 36-43, 2018y, URL:

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8334918&isnumber=8334903

5.   Rakhmonov O. Sh., "Common and different aspects of security protocols used in 4G and 5G networks", Proceedings of the international scientific and technical conference on the role of digital technologies in the development of exact sciences: problems and innovative solutions, 2024y: [318-322].

6.   Umarov Sh., Rakhmonov O., "5G communication network capabilities and role in data protection", International scientific and technical conference "Scientific basis of prospective application of innovative technologies in information communication", 2024: [392-397].