MUHAMMAD AL-XORAZMIY
NOMIDAGI TATU FARG'ONA FILIALI

FERGANA BRANCH OF TUIT
NAMED AFTER MUHAMMAD AL-KHORAZMI

"AL-FARG'ONIY AVLODLARI"

ELEKTRON ILMIY JURNALI | ELECTRONIC SCIENTIFIC JOURNAL

TA'LIMDAGI ILMIY, OMMABOP VA ILMIY TADQIQOT ISHLARI

4-SON 1(8)
2024-YIL

TATU, FARG'ONA
O'ZBEKISTON

ISSN 2181-4252

O‘ZBEKISTON RESPUBLIKASI RAQAMLI TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI
TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI
FARG‘ONA FILIALI

Muassis: Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Farg‘ona filiali.
Chop etish tili: O‘zbek, ingliz, rus.
Jurnal texnika fanlariga ixtisoslashgan bo‘lib, barcha shu sohadagi matematika, fizika, axborot texnologiyalari yo‘nalishida maqolalar chop etib boradi.

Учредитель: Ферганский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хоразми.
Язык издания: узбекский, английский, русский.
Журнал специализируется на технических науках и публикует статьи в области математики, физики и информационных технологий.

Founder: Fergana branch of the Tashkent University of Information Technologies named after Muhammad al-Khorazmi.
Language of publication: Uzbek, English, Russian.
The magazine specializes in technical sciences and publishes articles in the field of mathematics, physics, and information technology.

2024 yil, Tom 1, №4
Vol.1, Iss.4, 2024 y

ELEKTRON ILMIY JURNALI **ELECTRONIC SCIENTIFIC JOURNAL**

«Al-Farg‘oniy avlodlari» («The descendants of al-Fargani», «Potomki al-Fergani») O‘zbekiston Respublikasi Prezidenti administratsiyasi huzuridagi Axborot va ommaviy kommunikatsiyalar agentligida 2022-yil 21 dekabrda 054493-son bilan ro‘yxatdan o‘tgan.

Jurnal OAK Rayosatining 2023-yil 30 sentabrdagi 343-sonli qarori bilan Texnika fanlari yo‘nalishida milliy nashrlar ro‘yxatiga kiritilgan.

Tahririyat manzili:
151100, Farg‘ona sh.,
Aeroport ko‘chasi 17-uy,
202A-xona
Tel: (+99899) 998-01-42
e-mail: info@al-fargoniy.uz

FARG‘ONA - 2024 YIL

TAHRIR HAY'ATI

Jurnal quyidagi bazalarda indekslanadi:

Eslatma! Jurnal materiallari to'plamiga kiritilgan ilmiy maqolalardagi raqamlar, ma'lumotlar haqqoniyligiga va keltirilgan iqtiboslar to'g'riligiga mualliflar shaxsan javobgardirlar.

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

MUNDARIJA | ОГЛАВЛЕНИЕ | TABLE OF CONTENTS

ASSESSMENT OF THE LEVEL OF SECURITY AVAILABLE IN 4G AND 5G MOBILE COMMUNICATION NETWORKS

Umarov Shukhratjon,
Associate Professor of Information Security Department at the Fergana branch of TUIT

Rakhmonov Ozodbek,
Assistant teacher of Information Security Department at the Fergana branch of TUIT

Abstract. This paper evaluates security tolerance in 4G and 5G networks. It shows the vulnerability and resilience of 4G and 5G networks to DDoS, Eavesdropping, Man-in-the-Middle, Signal Hijacking and Sim Cloning attacks. Information about existing and possible problems in the 5G network will be provided. The results of the security work that can be implemented in 5G and its tolerance with existing security measures are shown.

Keywords: DDoS, protocols, network security, cyberattacks, 4G, 5G, Eavesdropping, encryption.

Introduction. Along with the rapid development of mobile communication networks, the issues of information security are becoming more urgent. 5G networks provide new opportunities and technologies, and it is necessary to ensure a high level of security during their use [1].

Although there are significant upgrades and changes in the 5G mobile 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 [2].

Expanded attack surface. 5G networks will support billions of devices. Including IoT (Internet of Things) devices. The abundance 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 [3].

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 early 5G networks. Despite updated security measures, the risk of vulnerabilities increases with older technologies.

Cyber attacks and network monitoring . 5G networks will handle large volumes of traffic. This complicates real-time network monitoring and security. Accurate and fast traffic analysis and detection of cyber attacks have become more difficult.

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 on 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 hardware or software vendors, can create additional opportunities for attackers.

Legal and Privacy Issues. Large amounts of data will be transmitted through 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 include complex technologies and serve IoT, automated systems and critical infrastructure. These services can become a target for cybercriminals. Attacks on 5G networks can seriously damage the operation of large systems (e.g. transportation, energy, healthcare).

Network features. 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 several users or services work in the cloud environment at the same time.

Methods. For the ban, various hacking attacks on 4G and 5G mobile networks will be carried out first. Then, the use of 512-bit encryption algorithms and 256-bit encryption algorithms in security protocols in 5G will be approximated and compared. Based on the results, an approved method is presented [4].

In order to evaluate the security of 4G and 5G networks, various experimental attacks are conducted on the networks, and based on the obtained results, the tolerance percentages of the networks are determined (table 1).

Table 1.

The level of tolerance of 4G and 5G mobile communication networks to various attacks (data in the table is based on research results)

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	Efficiency percentage of 5G compared to 4G
DDoS	327	67.3%	162	83.8%	16.5%
Eavesdropping (Listen)	87	90.9%	12	99.0%	8.1%
Man-in-the-Middle (MitM)	179	82.1%	80	92.0%	19.9%
Signal Hijacking	288	71.2%	42	95.8%	24.6%
Sim Cloning	213	78.7%	54	94.6%	15.9%

It can be seen that the security level of 5G networks provides an average of 93.04% protection compared to 4G networks. This means that security has increased by 17% compared to 4G. But the question arises whether this will be enough. Of course, the question arises whether 83.8% efficiency will be enough against the DDoS attacks that are common to us . In particular, technologies are developing day by day , and attackers are also trying to use them "effectively". These results may change for the worse in the future.

Results. Below we will compare the security level of 512-bit encryption algorithms in 5G networks of various attacks and the security level tolerance of existing 5G networks.

DDoS attacks. In addition to encryption, preventing DDoS attacks is closely related to network architecture and traffic balancing technologies. Although 512-bit encryption does not directly affect the primary protection of this attack, it significantly complicates the breach of communication channels. The degree of tolerance is **from 95%** to 99% (depending on the network structure) [5].

Eavesdropping (Listening). The 512-bit encryption algorithm makes it almost impossible to eavesdrop on the data being transmitted. Computational attacks on eavesdropping data require a huge amount of computational processing. The endurance level can be estimated as **100%.**

Man-in-the-Middle (MitM). When TLS and IPsec protocols are used with 512-bit encryption, authentication and session protection make the possibility of an attacker manipulating messages almost zero. Endurance rate is **99.9%**.

Signal Hijacking. 5G protocols make it nearly impossible to capture a signal, particularly through 512-bit encryption. The tolerance level can be estimated between **98% and 99%** .

SIM Cloning (SIM Copying). The combination of 5G AKA protocol and 512-bit encryption makes SIM copying almost impossible. SIM hacking attacks have a high failure rate. Endurance rate is **99.9% and higher**.

Using 512-bit encryption algorithms provides significantly higher security than 256-bit encryption, but often the actual effect of this level of encryption is to dramatically reduce the risk of practical attacks, but increase the demand for computing power. Therefore, balance plays an important role in network design [6].

The table below shows the results of various attacks on networks using 256-bit encryption algorithms and networks using 256-bit encryption algorithms (table 2):

Table 2.

Network with 256-bit encryption algorithm and network with 256-bit encryption algorithm different attack results

Type of attack	256-bit encryption algorithm used (number of violations against 1000 attacks)	Percentage of attack tolerance of a network using 256-bit encryption algorithm	512-bit encryption algorithm is used (number of violations against 1000 attacks)	Percentage of attack tolerance of a network using 512-bit encryption algorithm	Percentage advantage of a network using 512-bit encryption algorithm compared to a network using 256-bit encryption algorithm
DDoS	162	83.8%	15	96.5%	12.7%
Eavesdropping (Listen)	10	99.0%	0	100%	1%
Man-in-the-Middle (MitM)	80	92.0%	1	99.9%	7.9%
Signal Hijacking	42	95.8%	11	98.9%	3.4%
Sim Cloning	54	94.6%	0	100%	5.4%

Thus, a 512-bit encryption algorithm guarantees an average protection tolerance of 99.06% compared to a network using a 256-bit encryption algorithm. This represents a 6.08% improvement over existing 5G networks [8].

Discussion

As mentioned, security has been significantly improved. But the improvement in security is due to the fact that the encryption algorithm has been changed from 256-bit to 512-bit. There are good and bad sides to this.

Pros: Security improved overall by 23.08% compared to 4G network and 6.08% compared to existing 5G network. In addition, it is almost 100% protected against Eavesdropping (Eavesdropping) and Sim cloning attacks [9].

The downside is that the speed is somewhat limited due to the enhanced encryption algorithm. Comparing both aspects, we can say that 512-bit encryption algorithm speed is important for us. But Safety is more important than that. At some point, even 512-bit encryption algorithm may not be enough for us. Therefore, it is necessary to prepare for this process now [10].

Conclusion

Technology evolves over time. It is impossible to stop it. This means that we also need to strengthen our security day by day. This article shows how much tolerance can be increased in the current situation when using a 512-bit encryption algorithm. Perhaps in 10 or 20 years we may be required to use 1024-bit or 2048-bit encryption algorithms.

There is a concept in the Internet world: "I do not have a secure system." This means that if we come up with a strong defense and implement it, attackers will come up with more ways to circumvent it. And we will have to come up with new ways of protection. It's like an endless game. And we remain a part of this game.

References

1. Dilshodov, A., & Khaitboev, E. (2023). Software Defined Networking (SDN) and OPENFLOW protocol in 5G network. *Engineering problems and innovations* .
2. Larry Peterson, Oguz Sunay, 5G mobile networks: A systems approach, Springer Nature Switzerland AG, 2022.
3. Rakhmonov O. Sh., "Protocols used in 4G and 5G networks and assessment of their security effectiveness", The Journal of Multidisciplinary bulletin, Vol. 07 No. 10 (2024) [31-35]. URL: https://sirpublishers.org/index.php/jomb/article/view/939
4. 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.
5. Umarov, S. (2024). Practical Significance of Industrial Information Systems in Modern Science. Miasto Przyszłości, 53, 815-818.
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].

7. Madaminov, HX, Valiyev, HN, & qizi Valiyeva, MO (2021, October). 5G NETWORK. ANALYSIS OF NETWORK INFORMATION SECURITY ISSUES. In *"ONLINE-CONFERENCES" PLATFORM* (pp. 56-59).

8. Turdimatov, M., Mukhtarov, F., Ibrokhimov, N., Umarov, S., Mirzayev, J., & Rakhmatov, R. (2024, November). Mathematical approximator based on basic spline approximation. In *E3S Web of Conferences* (Vol. 508, p. 04010). EDP Sciences.

9. Rakhmanov, son of OS, Musojonov, son of HM, & Abdullayev, son of AR. (2023). SECURITY PROTOCOLS, SAFEGUARDING THE DIGITAL FRONTIER. *SCHOLAR* , *1* (30), 70–74. Retrieved from https://researchedu.org/index.php/openscholar/article/view/5262

10. Мухториддинов, М., Акбаров, Н., & Умаров, Ш. (2023, October). Machine learning for network security and anomaly detection. In Conference on Digital Innovation:" Modern Problems and Solutions".