Informatics

THE ROLE OF 5G TECHNOLOGY İN THE SECURİTY OF UAVs

Natiq Aliabbas Quliyev[1], Samira Hasan Gahramanova[2]

[1]Baku State University, Baku, Azerbaijan: natigguliyev@yahoo.com https://orcid.org/0009-0002-5116-5254

[2]Azerbaijan Technical University, Baku, Azerbaijan: samira.qahramanova@aztu.edu.az https://orcid.org/0009-0008-0319-9138

Abstract: In modern times, extensive applications of information technologies are observed in many areas. One of the latest applications of information technologies is unmanned aerial vehicles (UAVs). In this regard, optimal and safe management of UAVs is one of the most urgent issues of the modern era. The 3G and 4G mobile technologies that are widely used in modern times cannot fully ensure optimal and safe management of UAVs. In this regard, it is more useful to use the capabilities of 5G technologies, the new generation of mobile networks, to ensure uninterrupted and safe management of UAVs, because 5G mobile technologies have many positive new capabilities compared to LTE-based 4G technologies. From this point of view, the publication of this article is relevant.

Keywords*: unmanned aerial vehicles (UAVs), 4G networks, LTE, 5G networks, Low delay.*

Introduction.

Recently, in connection with the large-scale development of information technologies, many technologies of special interest have been applied to various fields of activity. One such interesting technology is unmanned aerial vehicles (UAVs).

Many countries consider the development and use of unmanned aerial vehicles promising. And there are many reasons for this. Because the drone needs almost none of the natural human needs. It can perform its duty around the clock with minimal interruptions for charging and maintenance. Words of encouragement are not essential for a drone; Even when a person is sleeping, the drone does not lose its vigilance. A drone can withstand loads that a human cannot. A program for a flying machine is a set of mandatory rules, and achieving the goal is only a matter of time [1,2].

In today's world, UAVs have become an increasingly important element of aviation technology, with applications ranging from military operations and surveillance to cargo delivery and search and rescue missions. With the development of communication technologies, new opportunities for control and monitoring of unmanned systems are emerging, which requires in-depth research and optimization of network technologies.

About the use of UAVs.

UAVs are often used in the military and intelligence fields, to obtain secret commercial information and classified information. Therefore, it is often used by various terrorist groups and criminal elements for selfish purposes. In this case, no one can be protected from disclosure of confidential information. These tiny flying robots were the weapons that disrupted two major oil refineries in Saudi Arabia in September 2019. Economic losses and human casualties are still difficult to calculate. In order to cause economic damage and create panic among the population, drones are mainly used to transport prohibited substances, obtain classified information and carry out attacks on large infrastructure enterprises. The small size of UAVs contributes to stealth, even with the use of special means, it is impossible to detect penetration into the protected area; At this time, radio-electronic complexes and jammers are most often used, which can affect the communication channels and interfere with the operation of the drone programmed for operation. Piloting of unmanned devices is mainly carried out using the following communication channels:

- Satellite navigation channels using GPS and GLONASS navigation systems;
- Channels for receiving and transmitting signals from the control element or operator console.

If you block or affect at least one of these channels, the drone will either lose orientation in space or return safely to the starting point due to a software failure. In this case, the goal cannot be further achieved.

The purpose of this article is to conduct research on the safe management of drone networks using 5G mobile communication technologies. These technologies promise significant improvements in data transmission, reduced latency, and increased reliability of communications that can be critical for effective control of unmanned systems in real-time.

UAVs are playing an increasingly important role in fields as diverse as logistics, environmental monitoring, agriculture, and information security. One of the main factors determining the effectiveness and reliability of the use of UAVs is the ability to control them reliably and quickly at long distances. Currently, fourth generation (4G) mobile technologies provide the necessary means to achieve this goal by providing high data throughput and low latency.

Classification of UAVs according to parameters.

Despite the fact that drones have only recently begun to be actively developed, there are already many classifications of them. We will look at only a few of them.

Depending on how management is carried out, UAVs are divided into [3, pp.1-33]:

- Uncontrolled (programmable) drones;
- Remotely controlled vehicles, devices;
- Fully automatic UAVs.

In the first case, a person only controls the launch of the drone and does not participate in the subsequent movements of the drone. For this, the necessary parameters are entered into the control panel and a flight program is created. And the pilot can only wait for the UAVs to bring the necessary information or to reach a conditional target (of course, if no UAV protection systems are used on the route).

In the second case, the operator has the opportunity to manually control the flight path and monitor the execution of the task..

In the third case, drone control does not require human intervention from start to finish.

Depending on the weight, drones are divided from the smallest to the very heavy.

Small drones are light, weighing up to 15 kilograms. Most of the time, battery charging lasts for 1 hour of flight. Small-sized drones weigh no more than 50 kilograms and can stay in the air for more than 4 hours. Giant-sized drones can weigh more than 1.5 tons and be completely autonomous.

According to their purpose, they classify commercial UAVs (for scientific purposes, research, servicing hard-to-reach equipment), hobbyist (for video shooting and competition) and combat UAVs (equipped with weapons and armor).

Depending on the design, drones consist of:

- Single rotor;
- Multi-rotor;
- Stationary, fixed-wing UAV;
- Hybrids of all of the above.

Technical characteristics of 4G networks for UAVs.

It should also be noted that 4G technology, which has found wide applications in modern times, has already proven itself to be an effective tool for controlling UAVs, providing high data transfer speed and low latency for the period of its operation, allowing to quickly control drones over long distances. With the emergence of 5G technologies, new horizons are opening to increase the functionality and efficiency of UAV network management. 5G provides significantly higher capacity, lower latency and the ability to connect a large number of devices, which is especially important for coordinating large fleets of drones.

Currently, fourth generation (4G) mobile technologies provide the necessary means to achieve this goal by providing high data throughput and low latency.

4G technology based on LTE (Long Term Evolution) standards offers a number of advantages for managing UAVs:

- **High data transfer rates**: 4G networks can provide download speeds of up to 100 Mbps and higher, enabling real-time video streaming and acquisition of sensor data onboard drones without significant latency.
- **Low delay**: Delay in 4G networks is typically around 30-50ms (Milliseconds), allowing control commands to be quickly transmitted to drones and responses received from drones.
- **Wide coverage and accessibility**: Currently, 4G networks are widespread and provide reliable coverage in both urban and rural areas, which allows UAVs to be used in a variety of conditions and environments...

Technical characteristics of 5G networks for UAVs.

5G technologies, which are the most modern mobile network technology in modern times, are planned to be widely applied in UAVs as well as in many modern fields.

5G technologies offer a number of key advantages for UAV control:

- **High data transfer speeds**: 5G networks can provide upload and download data speeds of up to 10 Gbps, enabling the transfer of large volumes of data, including ultra-high-definition video and real-time sensor data..
- **Low delay**: Delay in 5G networks is less than 1ms. This indicator is also quite low (30-50 times) compared to 4G technology. This is important for real-time management of UAVs and tasks that require an immediate response.
- **High connectivity density**: 5G technology supports the connectivity of up to one million devices per square kilometer, enabling large fleets of drones to be effectively managed in confined spaces..
- **High reliability and stability**: 5G networks provide a high degree of communication reliability and resistance to interference. Of course, this is also important for the safe and smooth operation of UAVs..

The introduction of 5G technology, which already has sufficiently high network performance, is inevitable. Providing very high data transfer speeds, extending coverage, increasing throughput, eliminating delay and significantly improving service quality are among the innovations of 5G technology. All this is happening thanks to the introduction of 5G technology. However, in addition to all these "good things", it is worth considering what security risks are associated with the use of 5G networks.

Expectations for 5G wireless networking are high. The fact is that 5G will be several times more efficient in processing more customers and therefore more data traffic than 4G. It is also worth remembering that this is a completely new technology that significantly contributes to the provision of modern services.

The advantages of 5G networks.

Currently, existing wireless network systems are clearly insufficient to meet user requirements. Therefore, the introduction of 5G networks is an immediate necessity! This will allow us to achieve 1-10 Gbps throughput by connecting 10-100 devices simultaneously. And all this will be accompanied by 100% transmission capability and 90% reduced energy consumption. Of course, this will be possible only with the integration of other technologies into 5G [4,5]:

- HetNet – heterogeneous networks.
- IoT – The Internet of Things.
- D2D – communication between devices.

- Device-to-Device (D2D) – communication between devices. Device-to-Device (D2D) – technology for direct communication between LTE standard devices appeared for the first time in the 12th edition of the 3GPP consortium and allows to increase the efficiency of the use of radio spectrum, increase the transmission capacity and reduce the energy consumption of user terminals. D2D enables the implementation of new peer-to-peer services and applications, but its main focus is on organizing public safety communication systems when the main network is unavailable or disrupted. At the same time, the implementation of D2D creates many challenges and risks for existing mobile communication architectures built around base stations.
- mMIMO – massively multiplexed output.
- mmWave – communication over millimeter waves (the advantages of 5G such as higher speed, greater throughput, greater network capacity and lower ping) are achieved using a wider frequency range than the previous generation. It is clear from a physics course that if the frequency is high, then the wavelength is also will be shortened. Frequencies between 24-300 GHz are called "millimeter waves" or mmWave. 26.50-29.50 GHz (n257) and 24.25-27.50 GHz (n258) are still reserved for mmWave technology. This type of 5G network is called “5G mmWave” or “High Speed 5G.” This type of network is deployed much slower than sub-6GHz, most mmWave stations are being developed in the US by the Verizon mobile operator.
- CRN – Cognitive radio networks
- CRAN – cooperative radio access network
- PUA – unmanned aerial vehicles network
- M2M – communication between machines (M2M or Machine-to-machine is a modern information technology based on the principles of interaction between two or more connected devices. In addition, communication can be based on wired or wireless communication. It is one-way or two-way allows information exchange, as well as tracking new information through a unified system.

5G technology means not only faster connections, but also innovative, revolutionary solutions that offer more possibilities. Remote operations or smart, secure neighborhoods are just some of the innovations on offer. The use of 5G networks mainly offers the following innovations:

- **Comfortable Internet without delay**. Thanks to 5G technology, we will be able to use the Internet very comfortably without any interference. Even if there are many users at home at the same time. With 5G, video conferencing, remote work and study, and most importantly, online gaming - all this can be done with very low ping and no delay.
  Note: Ping is the time required for a request sent to the network to reach the receiver and back. It is measured in milliseconds: the slower the Internet, the higher the ping. Also, ping is a console command that checks the quality of the Internet connection.
- **Very fast data transfer**. Today, 5G internet allows you to download files and data 10 times faster than 4G LTE. Live broadcasts, movies, series - all this can be watched in 4K quality without the problem of constant buffering.
- **Internet of Things (IoT) and VR**. It is clear that the 5G network provides a huge improvement. This is a technological breakthrough! We are able to connect more and more devices to our network. Home appliances (washing machines, refrigerators), traffic lights, autonomous vehicles and of course robots that will be connected to the 5G network. Of course, with the development of 5G technology, virtual reality (VR) is also developing. As a result, we will be able to remotely explore the city or "participate" in a sports match thanks to VR-glasses that will be connected to the 5G network.

The difference between 5G and 4G.

It should also be noted that the 5G network works on the same physical principles as the previous generation networks – 2G, 3G, 4G, that is, it also uses radio waves to transmit data and information. However, for the 100% implementation of the 5G network, it is necessary to reconstruct (improve) the existing infrastructure, as well as to build a new one. Base stations (antennas and transmitters) and backbone equipment must be restored. Then it will be possible to use higher frequencies (3.4 - 3.8 GHz and above) specially designed for 5G technology.

- **Comparison of data transfer speeds**. The idea of the 5G network is primarily to significantly speed up the mobile internet. This will allow us to download videos or send large files in seconds. Recall that LTE wireless Internet technology allows data transfer up to 300 Mb/s and up to 600 Mb/s with activated aggregation of 4G LTE bands, while the actual data transfer speed here is approximately 20-30 Mb/s does. This large reduction in actual throughput is closely related to factors such as terrain, buildings (attenuation), the number of people using a particular base station, or the capabilities of a smartphone or router. The technology of the 5G network provides data transfer even 10 times faster than 4G LTE, that is, the data transfer speed is increased to 20 Gbit/s.
- **Comparison of delays in data transmission**. 4G LTE networks have quite high latencies, these delays are 30-40 ms, and sometimes 100 ms. With 5G technology, delays will be reduced to 1-3 ms! This will allow the development of industries that are highly dependent on the Internet, such as the control of autonomous vehicles. The important role of 5G technology in the management of UAVs is also due to the fact that data transmission delays in 5G technology have decreased to 1-3 ms. This will lead to more efficient control of UAVs, especially in remotely controlled UAVs, the UAV will respond more effectively to the controller's commands. Delay is a term often used in the context of cybersecurity to describe the time that elapses between the initiation of an action and the response. This delay is common in network communications and has significant implications for both security and performance.
- **Comparison of high frequencies**. It should also be noted that in some places the 4G network operates at frequencies from 800 to 2600 MHz. The 5G network will use increasingly higher frequencies. The 5G network initially uses the 3.4 - 3.8 GHz bands. Finally, the 5G network will operate in the 26 GHz band.
- **Improved infrastructure of 5G networks**. The introduction of 5G networks is also related to modern infrastructure. Both base stations will be expanded and upgraded, and new transmitters will appear. This will allow to support a greater number of transmitting and receiving devices. Moreover, all this will happen without intervention.

Types of security threats in 5G networks.

Although the integration of all the above technologies has revolutionized modern wireless networks, we must also be aware of new security issues. In general, attacks on 5G networks are divided into two types:

- **Passive attacks**: Passive attacks involve the unauthorized use of information from authorized users that is not intended to disrupt communications. The most common types of passive attacks are traffic analysis and eavesdropping. In short, these are attacks related to the listening and analysis of network traffic. The attacker then tries to steal useful data messages that can be used for malicious purposes. A traffic analysis attack can also be used to steal encrypted signals from wireless radio networks.
- **Active attacks**: The goal of active attacks is to disrupt and change the communications and connections of authorized users. Examples of such attacks include congestion, denial of service (DoS), distributed denial of service (DDoS), and man-in-the-middle (MITM) attacks.
  - ✓ *Tampering*: Tampering attack is an attack that disrupts data transmission. These attacks are aimed at the physical layer of the network and are also the basis of DoS attacks.

Tampering attacks are very difficult to detect. It is able to intelligently adjust the jamming transmission power. Even if an attack is detected, it is still very difficult to mitigate its consequences.

- ✓ *Man in the Middle (MITM)*: This attack is an active type of attack where an attacker secretly takes control of the main communication channel between two legitimate users. MITM can be targeted at different levels of a communication channel to compromise confidentiality, availability, and privacy.

Security methods in 5G networks.

Of course, all threats to 5G networks can be addressed in one way or another. Many security architectures are currently offered. They are based on two types of security methods: cryptographic methods and physical layer security (PLS- Physical Layer Security) methods [6].

- **Cryptographic methods**: These methods are used at different levels of the 5G network architecture to combat security breaches. These methods are further divided into two types: Symmetric key cryptography is based on the concept of sharing a secret key between authorized users for encryption and decryption. The second type is asymmetric key cryptography, which uses a public key to encrypt data and a private key to decrypt it.
  The public key is shared with all communicating parties on the network, and each user has a unique private key. The performance of this cryptographic technique is highly dependent on the length of the key and the complexity of the algorithm. Obviously, the more complex the algorithm, the higher the performance and security. But such complex algorithms require more time and energy.
- **Physical layer security**: This technology provides higher security with less complex mechanisms and less latency and power consumption. The PLS (Physical Layer Security) method exploits the properties and defects of wireless channels such as noise, fading, interference, scattering, and diversity. PLS guarantees high security of user data, even if the legitimate user's channel is in worse condition than the listening channel. PLS methods for protecting the privacy of the wireless medium of data transmission include:
- Artificial sound injection;
- Preparation of signals to protect against eavesdropping;
- Secure beamforming/precoding;
- Secure cooperative transmission methods;
- Resource distribution and energy management.

Cyber security specifics of 5G.

In order to protect 5G networks from hacker attacks, cyber security technologies must improve significantly. Some security issues in 5G networks are related to the network itself, while others are related to the devices connected to it. Both can pose risks to consumers, businesses and government agencies.

Let's consider the main problems of information security in the new generation 5G networks [6].

Decentralization of security. Previous generations of networks before 5G had fewer physical interconnects, making it easier to maintain their security and performance. Dynamic software-based 5G systems require more routing points. Each of them should be checked regularly to ensure safety. It may seem complicated, but even one unsecured partition can compromise the security of the rest of the switching network components.

High throughput requires consideration of security techniques. Modern networks are limited in speed and performance, making it easy for providers to monitor the level of network security in real time. Therefore, the advantages of the extended range of the 5G network can also compromise its security. Developers will have to think of new ways to deal with modern threats.

Many IoT devices are not provided with security tools, features. Not all manufacturers make cybersecurity a priority, and this is especially true for budget smart devices. 5G opens up new opportunities for using the Internet of Things. The variety and number of devices connected to the network is increasing, but more security options mean more hacking options. Small devices like smart TVs, door locks, refrigerators, speakers, and even aquarium thermometers can become weak points in your network. The lack of a security standard for IoT devices can lead to an active increase in the number of cybercrimes.

The lack of encryption when establishing a connection opens up access to information about a device that criminals can use to target such a device through an IoT connection. By capturing unencrypted data, attackers will know exactly which devices are connected to the network. By knowing the operating system and type of device (smartphone, car router, etc.), attackers will be able to plan their attacks more precisely.

Device vulnerabilities are used for various attacks. Let's mention some of the main ones.

- Botnets control networked devices for massive cyber attacks.
- DDoS attacks overload a network or website and block its access to the Internet.
- A man-in-the-middle attack (MiTM-attack) is the undetected interception and alteration of messages exchanged between two parties.
- Location tracking and call interception are no problem for those with a little knowledge of paging protocols in broadband systems.

The impact of delay on cyber security.

One of the factors that play a key role in cyber security in modern times is the delay in data transmission in the network. The role of latency in cyber security is that it is essential for implementing effective measures to protect network systems. Among the cyber-attacks and cyber-threats that can be caused by the delay in the network, especially in the mobile network, we can mention the following:

Network attacks. Delay can be used by hackers, attackers to perform timing, time-based attacks, such as temporal attacks. These attacks analyze response latency to gain valuable information about system vulnerabilities. By closely monitoring the time it takes for a system to respond to certain requests, attackers can identify weaknesses and potentially exploit them for unauthorized access or data theft.

Data theft. Delay can also affect data transfer speeds, making it easier for cybercriminals to intercept sensitive data during communication delays. When data is transmitted more slowly due to latency, it gives attackers more time to intercept and compromise data. This highlights the importance of using secure communication channels and encryption protocols to protect sensitive data in transit.

Denial of Service (DoS) attacks. Denial of Service (DoS) attacks aim to disrupt the normal operation of a network or system by overloading it with excessive traffic. Delay can play a significant role in this scenario. Attackers use delay to flood the system with a large number of requests, thereby consuming its resources and causing performance bottlenecks. By exploiting the delay, attackers can amplify the effects of DoS attacks, effectively rendering the target system unavailable or severely degraded.

Cloud Security. Delay in cloud computing environments can directly affect the response of security measures. If delay is not managed effectively, delays in detecting and responding to threats can occur in such environments. For example, if a security tool takes longer to analyze network traffic due to delay, it may be slower to identify and remove potential threats. As organizations increasingly rely on cloud services, managing latency becomes essential to maintaining effective security measures.

Conclusion.

As can be seen from the research in the article, one of the most important measures to prevent cyber attacks in any area where wireless networks are applied, including UAVs, is to adjust network delays. It is by reducing the latency of wireless networks that many potential cyber-attacks can be prevented, thereby ensuring the safe operation of sufficient UAVs. In this article, we also investigated that 5G technologies can ensure the maximum reduction of delays in wireless networks, as this is due to its technical indicators. It should also be noted that in 5G technologies, reducing delays in wireless networks can also be achieved through cryptographic methods and physical-level security. In this regard, the application of 5G technologies in UAVs can be considered the most optimal solution to reduce existing cyber attacks on UAVs and for its safe and operational management in general. Of course, the other positive advantages of 5G technology that we mentioned in the article also play an important role in ensuring the safe and prompt operation of UAVs.

REFERENCES

1. Quliyev N.A. 5g technologies are entering a new era in medical science. Proceedings of the 8th International Scientific and Practical Conference. Science and practice: implementation to modern society. Manchester, GREAT BRITAIN №3 (39) (2020), pp.1711-1723.
2. Quliyev N.A., Shamilov Z.A., Applications of 5G technology in agriculture. II International scientific and practical conference. Global and regional aspects of sustainable development. COPENHAGEN, DENMARK. № 43 (2021), pp.642-648.
3. Ghamari, Mohammad, et al. "Unmanned aerial vehicle communications for civil applications: A review". IEEE Access 10 (2022): 102492-102531. 42 p.
4. Quliyev N.A. 5G technologies are creating a new world order. Norwegian Journal of development of the International Science. ISSN 3453-9875. №82/2022. Iduns gate 4A, 0178, Oslo, Norway., pp.62-68.
5. Quliyev N.A., Shamilov Z.A., Kahramanova S.H. About the Interaction of Artifical Intelligence and 5G technology. X International Scientific and Practical Conference CHALLENGES IN SCIENCE OF NOWADAYS, November 16-18, 2022 in Washington, USA., pp.456-465.
6. 5G; Security architecture and procedures for 5G System. https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf, 251 p.

Accepted: 21.05.2025