Baku State University Journal of Mathematics & Computer Sciences ***2024****, v.1 (3), p. 51-68*

journal homepage: http://bsuj.bsu.edu.az/en

THE USE OF 5G TECHNOLOGY IN ENSURING THE CYBER SECURITY OF UAVs

Natiq A. Quliyev, Samira H. Kahramanova, Sadig N. Samadov

Baku State University, Azerbaijan Technical University, British School in Baku
Received 10 may 2024; accepted 28 august 2024

https://doi.org/10.30546/209501.101.2024.1.3.068

Abstract

In the article, the comparison of the capabilities of 5G networks, which are planned to be widely used, in the management of UAVs, with the currently widely used 4G mobile network technologies was considered. Since both 5G technology and UAVs are new applications of information technology, and especially the recent wide application of UAVs, the secure management of UAVs and 5G networks is one of the most pressing issues. Considering this point of view, it is actually to publish this article.

Keywords: unmanned aerial vehicles (UAVs), 4G networks, LTE, 5G networks, Low delay
Mathematics Subject Classification *(2020):* 34A30, 34B09, 34B15, 34C23, , 47J10, 47J15

1. 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).

In the world, the demand for unmanned aerial vehicles is increasing. This is related to its wide applications in many fields. Productivity of UAVs is much higher

than devices operating with direct human participation. From this point of view, the production and use of UAVs is considered a promising field. In particular, the fact that the drone needs almost none of the natural human needs makes its use even more relevant. Unmanned aerial vehicles can easily cope with tasks that are beyond the capabilities of humans. In the control of drones, a person simply defines the software and action plan that ensures its control.

In today's world, unmanned aerial vehicles (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.

The fact that UAVs usually have small dimensions makes them an indispensable tool for covert operations, they help in a kind of stealth, even when using special tools, it is impossible to detect penetration into a 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.

It is necessary to block or affect at least one of these channels in order to change the spatial orientation of the UAV or to disrupt its program activity in general.

The purpose of this paper is to conduct research on the safe management of drone networks using 5G mobile communication technologies. In addition to being a new mobile network technology, 5G technologies offer many new opportunities. These technologies provide significant improvements in data transmission, reduced latency, and increased reliability of communications, which can be critical for effective control of unmanned systems in real-time. It is these new capabilities that make 5G technologies an important tool in the management of UAVs.

Unmanned aerial vehicles (UAVs) play an increasingly important role in various fields such as environmental monitoring, logistics, agriculture, and information security [6]. 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. The currently widely used fourth generation (4G) mobile technologies provide the necessary means to achieve this goal by providing high data throughput and low delay.

Despite the fact that UAVs are one of the latest achievements of information technology, since UAVs have found very wide applications, their security issue has come to the fore. As UAVs find widespread applications, their security risks have also begun to increase, and sometimes cyber attacks against UAVs have already taken place. Especially after Iran successfully hijacked the US RQ-170 drone through global positioning system (GPS) spoofing technology in 2011, more and more attacks on UAVs appeared, and the issue of UAV cyber security became more and more urgent [2].

The security of UAVs is not only about its own protection. The security issue of UAVs includes attacks on the network it is controlled by, its software, intellectual applications and control algorithms. These attacks can compromise the privacy, integrity and availability of the UAV, in some cases causing data loss and in some cases causing serious damage.

Nowadays, many experts classify UAV security threats into four categories: communication network security, software security, payload security, and intellectual security [2]. In this article, the security of the communication network in which it is controlled, which creates the greatest security risk for UAVs, is investigated.

2. Classification of UAVs according to parameters

Despite the fact that UAVs are basically one of the latest achievements of modern information technologies, 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:

- Uncontrolled (programmable) drones;
- Remotely controlled vehicles, devices (Picture 1);

- Fully automatic UAVs.

In the first case, the operator controls the flight path manually and has the ability to monitor the execution of the task.

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

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

Picture 1. Remotely controlled vehicles in "Technoxian" world robot championship (Baku).

UAVs also differ in weight. 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 the following [1]:

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

3. Capabilities of 4G networks for the operation of UAVs

It should also be noted that 4G mobile network technology is widely used in modern times and is widely applied in many fields. 4G mobile technology has also proven to be an effective tool for self-piloting UAVs. 4G networks provide high data rates and low latency for the duration of their operation, allowing for rapid control of UAVs over long distances. 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:

- 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.
- High data transfer speeds: 4G networks can provide download speeds of up to 100 Mbps and higher, enabling real-time video streaming and acquisition of sensor data on-board drones without significant delay..
- 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.

4. Technical characteristics and advantages of 5G networks for UAVs

Numerous new capabilities of 5G technologies have also led to the emergence of new opportunities to increase the functionality and efficiency of UAV network management. Therefore, 5G technologies, which are the most modern mobile network technology, are planned to be widely used in UAVs as well as in many modern fields.

5G technologies offer a number of key advantages for the optimal management of UAVs:

- High speed of data transmission: One of the main advantages of 5G technology is that it provides high speed of data transmission. 5G networks can provide data upload and download speeds of up to 10 Gbps, enabling the transfer of large volumes of data, including ultra-high-definition video and real-time sensor data.
- High connectivity density: 5G technology also enables high connectivity of a large number of devices to the network. 5G technology supports up to one million devices per square kilometer, allowing large fleets of drones to be effectively controlled in confined spaces.
- Low delay: One of the main advantages of 5G technology is that it minimizes delays in information exchange. 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 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 optimal operation of UAVs.

The high-quality indicators provided by 5G technology in the field of mobile networks determine its wide application in modern times. Providing very high transmission speeds, extending coverage, increasing throughput, eliminating latency, and significantly improving service quality make 5G technology inevitable to be applied in the UAV industry as well.

On the other hand, expectations for 5G wireless technology are high. The fact is that 5G is considered to be several times more efficient in processing more customers and therefore more data traffic.

It should also be noted that existing wireless systems, such as 4G, are clearly

insufficient to meet certain user requirements, especially in the field of UAVs. Therefore, the implementation of 5G networks is of particular importance. This will allow us to achieve 1-10 Gbps throughput by connecting hundreds of devices to the network at the same time. 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. Among such technologies, we can show the following:

- HetNet - Heterogeneous networks,
- IoT - The Internet of Things,
- D2D - Communication between devices
- M2M - Communication between machines,
- mMIMO - Massively multiplexed output,
- mmWave - Communication over millimeter waves.
- CRN - Cognitive radio networks,
- CRAN - Cooperative radio access network,
- PUA - Unmanned aerial vehicles network.

The innovations of 5G technology are not only about high-speed connections, but also about innovative, flexible solutions that offer more possibilities. For example, remote operations or smart, secure spaces 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, most importantly - online games - 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. It also paves the way for a technological breakthrough. We are able

to connect more and more devices to our network. Household 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 match thanks to VR-glasses that will be connected to the 5G network.

5. **Comparison of 5G and 4G**

It should also be noted that 4G and 5G networks have some common features. For example, 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 full functioning and implementation of the 5G network, it is necessary to reconstruct (improve) the existing infrastructure, as well as to build a new one. For example, base stations (antennas and transmitters) and backbone equipment must be rebuilt. After that, it will be possible to use higher frequencies (3.4 - 3.8 GHz and above) specially designed for 5G technology.

Comparison of transmission 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 at speeds up to 300 Mb/s and up to 600 Mb/s (LTE cat.12) with activated aggregation of 4G LTE bands, while the actual data transfer rate here is approximately 20 -30 Mb/s. 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 5G network should provide data transfer even 10 times faster, that is, the data transfer rate should reach 20 Gbit/s.

Comparison of delays in data transmission. The currently widely used 4G LTE networks have quite high delays, these delays are 30-40 ms, and sometimes 100 ms. With the full implementation of 5G technology, delays are reduced to 1-3 ms. This will allow the extensive development of industries that are directly 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 a network action and the response. This delay is common in network communications and has significant implications for both security and performance.

Comparison of higher 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. 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.

5G technology, in turn, improves 4G services in several ways. These directions mainly consist of the following:

Enhanced mobile broadband (eMBB) access: Here a higher speed of data transmission is defined. It offers up to 50 Mbps for outdoor use for downlink and 1 Gbps for indoor (5GLAN), half of these prices are available for uplink. A number of case studies are reviewed, including aviation - where eMBB helps deliver 1.2 Gbps bitrates to air traffic. creates an impossible opportunity. Of course, this also creates an irreplaceable opportunity for UAVs for its security and optimal management compared to 4G.

Critical Communications (CC) and Ultra Reliable and Low Latency Communications (URLLC- Ultra Reliable and Low Latency Communications): Here, even in some contexts, extremely high reliability is expected. For example, for remote control of process automation, the user expects 99.9999% reliability with a data transfer rate of up to 100 Gbit/s and a latency of 1-3 ms. This is especially enabled through Edge Computing capabilities.

Note: The concept of edge computing has arisen due to the exponential growth of IoT devices connecting to the Internet to either access data from the cloud or deliver data back to the cloud. And many IoT devices generate enormous amounts of data during their operations that are essentially

useless after processing.

Edge computing hardware and services help solve this problem by providing a local source for processing and storing data for many of these systems. For example, an edge gateway can process data from an edge device and then send only the required data back through the cloud, reducing the need for communication channel bandwidth. Or it can send data to an external device as needed with real-time application.

Massive Internet of Things (mIoT). Several scenarios require the 5G system to support very high traffic densities of devices. The Massive Internet of Things requirements include the operational aspects that apply to the wide range of IoT devices and services anticipated in the 5G timeframe.

Flexible network operations. These are some of the key features offered by the 5G system. It covers aspects such as network severance, network capability exposure, scalability and various mobility, security, effective content delivery, migration and interoperability.

6. **Mechanism of trust model in network**

One of the factors that ensure security in the network is the reliability model. The trust model defines the rules and mechanisms for verifying digital signatures and ensuring the security of communication in the digital environment. Trust models define how trust is established and maintained across entities in a digital ecosystem.

The reliability model also changes when moving from a non-autonomous system to an autonomous 5G system. Trust in the network is considered to decrease with distance from the core. This, in turn, affects decisions when developing a 5G security system.

The trust model in UE is quite simple. There are two domains of validity:

1. UICC (Universal Integrated Circuit Card), which houses the USIM (Universal Subscriber Identity Module) card, a universal internal card protected from unauthorized access.
2. Mobile Equipment (ME)

ME and USIM together form the UE.

In roaming and non-roaming cases, the network-side trust model differs accordingly. Here, trustworthiness is demonstrated on many levels that are

integrated into one another..

The radio access network (RAN- Radio Access Network) is divided into distributed units (DU- distributed units) and central units (CU- central units). Here, DU and CU together form the 5G base station gNB. DU has no way to contact customers as it may be hosted on unmonitored sites. The CU and Non-3GPP interoperability function (N3IWF - not shown in figures) which concludes the security of the Access Stratum (AS- Access Stratum) are deployed at sites with more limited access.

The Access Management Function (AMF) completes the security of the non-access stratum (NAS- Non-Access Stratum) in the core network. In the 3GPP 5G Phase 1 standard, AMF is combined with a Security Anchor Function (SEAF-Security Anchor Function), which contains the master key ("anchor key") for the visited network.

Authentication Server Function (AUSF) reuse when the key obtained after authentication is simultaneously registered in different network access technologies of the UE, such as 3GPP access networks and Non-3GPP access networks such as IEEE 802.11 (WLAN) wireless LAN saves for The Authentication Credential Repository and Processing Function (ARPF) stores the authentication credentials. This is reflected on the client side, i.e. UE side, with the help of USIM. Subscriber data is stored in a unified data repository (UDR- Unified Data Repository). Unified Data Management (UDM) uses data stored in UDR and creates registration data for authentication, user identification, session persistence, etc. implements application logic to perform various functions such as here, active and passive attacks through the cloud service are considered at both the management and user levels. In a roaming architecture, the home and guest networks are connected through an edge network function (Security Edge Protection Proxy- SEPP) to manage the communication plane. This enhancement was implemented in 5G networks due to the number of attacks detected in SS7, such as key theft and routing attacks, as well as host (network node) impersonation and source address spoofing in DIAMETER signaling messages, which exploit the secure nature of network interactions.

Note: Diameter is a protocol that provides authentication data exchange services, network access applications, and authorization for data mobility in 3G, 4G, IMS, and LTE networks.

7. Security capabilities of 5G technology

As we mentioned, 5G is implemented in several stages. Therefore, the security of 5G networks is wide-ranging. The 3GPP consortium has published 5G Phase 1 Security (Release 15), which characterizes the capabilities of 5G technology mainly in terms of security. This release is a fully specified system as of September 2019. Release 15 defines phase 1 of 5G, which introduces new radio transmission techniques and other key concepts such as certain levels of reliability, enhanced modularity or faster response times.

Fifth generation mobile telephony, or 5G or 5GS, was defined by the 3GPP consortium in release 15.:

The 5G Phase 1 document brought quite a few innovations and improvements compared to 4G LTE security. Let's mention these innovations below.

Initial authentication. In the 5G network, device authentication is based on initial authentication. It is similar to that used in 4G, but with some differences. Here, the authentication mechanism has built-in home control and allows the home operator to know whether a device is authenticated on a given network and accept the last authentication challenge. In Phase 1 of 5G technology, there are two important authentication options:

- authentication and coordination of 5G (5G-AKA) keys;
- Extended authentication protocol EAP-AKA.

Note: 5G-AKA (5G Authentication and Key Agreement) is an agreement for mutual authentication between UEs and the network. It is an enhanced packet and key agreement (EPS-AKA) for mutual authentication between 4G UEs and the network.

It should also be noted that 5G technology enables other authentication mechanisms based on EAP. In addition, pre-authentication does not depend on the radio access technology, so it can also work with technologies such as IEEE 802.11 WLAN other than 3GPP.

Note: EAP (Extensible Authentication Protocol) is an extensible authentication protocol or infrastructure that defines a sending format and is described by RFC 3748, often used in wireless networks and point-to-point connections. WPA and WPA2 standards support five types of EAP as the official authentication infrastructure (there are about 40 types of EAP in total); For wireless networks, EAP-TLS, EAP-SIM, EAP-AKA, P EAP, LEAP and EAP-TTLS are

suitable.

Secondary authentication. In 5G, secondary authentication is intended for authentication on data transmission networks outside the domain of the mobile operator's network. Various EAP-based authentication methods and corresponding registration data can be used for this purpose. A similar service was available in 4G, but now it is integrated into the 5G architecture.

Security between operators. In previous generations of mobile communication systems, there are several security issues at the inter-operator interface that arise from the SS7 or Diameter protocols. This problem has also been solved by 5G technology. 5G Phase 1 ensures security between operators from the start.

Confidentiality. Subscriber authentication issues have been known since 4G and previous generations of mobile systems. 5G has developed a privacy solution that protects the user's persistent ID from active attacks. Here, the public key of the home network is used to ensure the confidentiality of the subscriber's identity.

8. **The impact of delay on cyber security**

The role of delayy in cyber security is that it is essential for implementing effective measures to protect network systems. Here's a look at a few types of attacks that delay can create:

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.

Latency can play a significant role in this scenario. Attackers use latency 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 effectively managed, 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 latency, 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.

9. The role of the level of application of 5G technology in the mobile network in its security

It should also be noted that when examining security issues in 5G technology, it is also necessary to examine its architecture and, in particular, its specific application. It is at this point that the appropriate rules of the 3GPP consortium should be followed.

3GPP (3rd Generation Partnership Project) is a consortium that develops specifications for mobile telephony. 3GPP was established in 1998.

The main activity of the 3GPP consortium is the development of specifications and technical reports in the field of network technologies and radio access in mobile systems. 3GPP is also the general term for a number of standards organizations that develop protocols for mobile communications.

In this regard, the 3GPP consortium defines the standards for 5G as well. According to 3GPP, the 5G system (5GS) will consist of three main components.

1. User Equipment (UE),
2. 5G Radio Access Network (5G-RAN),
3. 5G base network (5GC).

UEs are devices (user equipment) that support 5G. 5G-RAN (also known as gNB) is a type of network infrastructure used for mobile networks, typically consisting of radio base stations with large antennas. RAN wirelessly connects

user equipment to the core network. The 5G core network simplifies various network functions such as session management, authentication, policy control, data storage, etc. There are several open source 5G core network implementations available. Free5GC, Open5GS are two of the most popular 5G core network implementations.

The 3GPP consortium mainly proposes two modes for the implementation of 5G technology: autonomous (Standalone-SA) and non-autonomous (non-standalone-NSA) network modes.

Note: 5G's autonomous (Standalone-SA) network mode includes all the capabilities of 5G. It is in them that the full potential of 5G can be realized: high signal delay (from 1 to 10 ms), mass connection of devices to one base station (up to 1 million per square kilometer), "network slicing", VoNR and other new services.

In 2020-2021, Non-Standalone (NSA) networks, which began to spread around the world, are mainly based on the previous generation 4G communication. In fact, they are a switching infrastructure, where only one advantage of the fifth generation is realized - high data transfer speed. When making a voice call in NSA mode, the subscriber is "moved" to the 4G base network.

In general, the implementation of the 5G standard is a multi-stage process. Usually, for the convenience of mobile operators, the first 5G networks can be created on top of the 4G infrastructure in the so-called "non-standalone mode" (NSA) mode. In this approach, the new 5G technologies provide high data transfer speeds, but use the existing 4G network to manage the connection at a lower level.

In this regard, the first step taken by the 3GPP consortium towards the implementation of 5G was the non-standalone mode (Non-Standalone - NSA) known as EN-DC (E-UTRA-NR Dual Connectivity). A key feature of non-autonomous mode is the ability to use pre-existing LTE infrastructure to make new radio technology available without changing the network.

EN-DC uses LTE as the primary radio access technology, and secondary radio access technology with User Equipments (UE) as the new radio access technology (New Radio-NR) access technology serves. The security procedures for EN-DC are

basically the same as the dual connection security standards for 4G.

The NSA transition period to 5G networks also typically reduces operator costs and allows for 5G network deployment in multiple phases. At the same time, the 5G network operating in a non-autonomous mode is limited in some of its capabilities. In particular, minimum delay in 5G networks is possible only when using standalone mode (SA).

Security of non-autonomous networks. The eNB station, which is the primary base station of the LTE standard network, checks whether the UE has 5G NR capabilities and gNB access rights to access the secondary gNB, that is, the 5G base station.

Note 1: eNB (Evolved Node B) is a type of mobile base station used in LTE (Long-Term Evolution) networks.

Note 2: 5G-RAN (also known as gNB) is a type of network infrastructure used for mobile networks, typically consisting of radio base stations with large antennas. RAN wirelessly connects user equipment to the core network. The 5G core network facilitates various network functions such as session management, authentication, policy control, data storage, and more. There are several open source implementations of the 5G core network. Free5GC, Open5GS are the two most popular 5G backbone applications.

The base station eNB generates and sends a key to be used by the gNB for secure communication via NR; The UE also receives the same key. In contrast to dual connectivity in 4G networks, Radio Resource Control (RRC) messages can be exchanged between the UE and the gNB, with keys used to protect the integrity and confidentiality of RRC messages as well as User Plane (UP) data. is obtained. Although UP data integrity protection is supported in 5G, it will not be used in EN-DC case.

Conculision

As the research in this article shows, many cyberattacks on networks, especially mobile networks, are caused by network delays. In this regard, one of the most important measures to prevent cyberattacks in any area where wireless networks are applied, including UAVs, is the regulation of 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 provide the maximum reduction of delays in wireless networks, as it is related to its technical performance. In this regard, the application of 5G technologies in UAVs can be considered the most optimal solution for reducing existing cyberattacks against UAVs and for its safe and operational management in general. Of course, the other positive advantages of 5G technology mentioned in the article also play an important role in ensuring the safe and efficient operation of UAVs.

In the article, we also investigated that the minimal delay factor, which plays an important role in the cyber security of UAVs, is possible only during the application of 5G networks in standalone mode (Standalone-SA). In this regard, in order to optimally and safely control the operation of UAVs, it is necessary to use only the independent mode of 5G networks (Standalone-SA) when using 5G.

It is obvious that most of the cyberattacks happen by breaking the authentication process in the network. Sometimes it is widely used in attacks on authentication protocols. As we mentioned in the article, the best authentication tools and methods are also available in 5G networks. In this regard, the application of 5G networks is very important for the safe and optimal management of UAVs.

References

[1] Ghamari, Mohammad, et al. "Unmanned aerial vehicle communications for civil applications: A review." IEEE Access 10 (2022): 102492-102531.

[2] Wang, Zhaoxuan. A survey on cyber security attacks and defences for unmanned aerial systems. https://www.sciencedirect.com/science/article/abs/pii/S1383762123000498

[3] 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

[4] 5G networks and 3GPP Release 15. https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2019/ITUPITA2018/ITU-ASP-CoE-Training-on-/5G%20networks%20and%203GPP%20Release%2015_vf.pdf

[5] 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/

[6] 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.

[7] 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.

[8] Quliyev N.A., Shamilov Z.A., Kahramanova S.H. About the Interaction of Artificial Intelligence and 5G technology. X International Scientific and Practical Conference CHALLENGES IN SCIENCE OF NOWADAYS, November 16-18, 2022 in Washington, USA.