UDC 621.391 doi: 10.20535/2411-2976.12024.18-27

AUTHENTICATION OF WIRELESS SYSTEMS BASED ON A DRONE SWARM AS A COMPONENT OF THE 5G RADIO ACCESS NETWORK ARCHITECTURE

Serhii O. Kravchuk, Iryna M. Kravchuk

Educational and Research Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. When establishing security measures for telecommunication networks involving unmanned aerial vehicles (UAVs), characteristics such as high scalability, device diversity, and high mobility should be considered. Authentication is a fundamental property that allows a UAV network to establish secure communication between its core components. Authentication also protects the UAV network from attackers impersonating legitimate UAVs. UAV authentication can further secure the communication channel by preventing impersonation and replay attacks. The design of UAV access control schemes, such as authorization and authentication mechanisms, remains a challenging research problem in UAV networks. The network becomes even more complicated when it interacts with a multitude of UAVs, called a swarm. A swarm by its very nature has a dynamic structure, and this raises the issue of unreliable constraints on UAVs in its composition. A standardized solution for the authentication of a single drone using the new 5G radio network (NR) is known, but for a swarm of drones, this is an open field of research. Per-UAV authentication key sharing as described in 5G NR does not scale across groups of UAVs.

Objective. The purpose of this work is to conduct an analytical review and consider approaches to creating procedures for the authentication of a swarm of UAVs/drones with wireless equipment on board for the 5G NR network, taking into account the features of swarm formation and the very requirements for 5G authentication.

Methods. Analysis of factors affecting the quality of provision of telecommunication services using UAVs in fifth generation networks. Analysis of well-known publications dedicated to the implementation of 5G networks and the use of drones in them. Comparing the implementation of UAV authentication procedures with on-board wireless equipment in the 5G network.

Results. The widespread use of small UAVs, as well as the large expansion of wireless 5G networks, requires new security measures to prevent unauthorized access to sensitive data.

Identification and Authentication for a mobile operator's network using drones allows for secure communication between its main components. This makes it possible to recognize the very drones that participate in the formation of such a network. Drone authentication often protects the communication channel by preventing replay attacks. The development of drone radio access control mechanisms, such as authorization and authentication mechanisms, remain relevant researches for the construction of promising radio access networks involving UAVs.

It has been confirmed that the introduction of special group procedures for the authentication of a swarm of drones in the 5G network can significantly improve the quality of the provision of telecommunication services.

Conclusions. When working with a swarm of drones, in addition to the usual problems with encryption and authentication (within the swarm and for communication between the swarm and the ground control station), there are additional problems related to the constant change in the composition of the swarm and its hovering position: drones can join or leave a swarm.

Depending on the swarm management structure, a different method of authentication will be needed, which makes it difficult to unify such procedures for a swarm of drones. Authentication procedures for a swarm of drones in 5G can be implemented through the following approaches: individual authentication, when each drone as a member of the swarm undergoes authentication with one NR 5G ground station; you can consider such an approach as authentication of a group of IoT devices, if the traffic of the swarm is very limited; group authentication through a leader drone that communicates with swarm members and the 5G operator's network; group distributed authentication through edge drones.

Group authentication via a drone leader is presented, where authentication is performed through a mechanism based on distributed delegation to reduce the service traffic directed to the 5G operator's core network. Here, legitimate drones are authorized as proxy delegated signers to perform authentication on behalf of the underlying network.

Group distributed authentication through boundary drones is considered, which offers more solutions than the case of authentication through a leader drone. Here, a solution is possible for several cases at once, for example, authentication of new drones (entering the swarm or leaving the swarm) and merging two separate drone swarms.

Keywords: *5G; NR 5G; security; authentication; group authentication; identification; drone; UAV; swarm of drones.*

I. INTRODUCTION

The development of modern electronic communications proceeds by increasing the mobility of the infrastructure itself for the provision of information services, which confirms the intensive development of cellular mobile communication networks of the 5th and 6th generations [1, 2]. One of the achievements of the development of the 5G mobile network is to go beyond the traditional approach of mobile broadband to expand the possibilities of providing new solutions that meet the urgent needs of the development of the modern heterogeneous infrastructure of electronic communications [3-5]. A good example of such a solution is the standardization work carried out in the Release 17 documents of the 3GPP (3rd Generation Partnership Project) organization (TS 29.255 and TS 29.256 specifications) regarding the use of cellular communication with the support of Unmanned Aerial Systems (UAS, Uncrewed Aerial Systems) on to the base of small unmanned aerial vehicles (UAVs) - drones, which allows the mobile operator's network to benefit from universal coverage, high reliability of connections, maintenance of service quality and dynamic mobility of nodes of its infrastructure [6, 7].

The widespread use of small UAVs for various applications, as well as the ubiquitous wireless connectivity of 5G and 6G networks, may require new security measures to prevent unauthorized access to sensitive data [8]. Similarly, when establishing security measures for networks with drones, one should take into account such characteristics as high scalability, variety of device implementations, and their high mobility [9].

Authentication is a fundamental characteristic that allows a drone network to establish secure communication between its core components. This allows for the authentication and identification of the drones themselves that participate in the formation of such a network. The security reliability of each drone is verified using a digital signature and only authenticated drones can continue to operate on the network. Authentication also protects the drone network itself from attackers who want to replace a working UAV.

Drone authentication can protect the communication channel by preventing repeat attacks. The development of drone network access control schemes, such as authorization and authentication mechanisms, remain relevant researches for the construction of various networks involving UAVs.

Known solutions for authenticating a single drone using the new 5G radio network (NR) require two steps. The first step covers the authentication between the drone and the 5G core network, and the second step covers the authentication between the drone and the drone control station. It is not possible to authenticate every drone in a swarm with the current solution without delay. The authentication keys between the base station (BS) and the user equipment (UE) must be transferred to the new BS during handover [10 - 12].

Groups of drones are very mobile and may require several switches from one BS to another BS. In a 5G NR radio access network for a group of drones, not necessarily a swarm, there may be a latency problem caused by authentication requests from the core network for each new connection. If the number of new members of the group is too large, the servers in the basic network may cause a delay, or even refuse to authenticate.

It is also important to consider some specific aspects of cooperation both within a drone swarm and between swarms, which are closely related to the authentication model and affect the algorithms underlying the execution of swarm missions. In addition to the usual encryption and authentication problems (within the swarm and for communication between the swarm and the ground control station), there are additional problems. Thus, a swarm by its nature has a variable structure, and this raises the problem of unreliable boundaries of such a swarm. In addition, the swarm is a system that constantly changes in its composition and position: drones can join or leave the swarm due to planned actions or due to unexpected events. An external drone can join the swarm instead of a drone leaving it. Thus, there will always be a threat of intrusion into a swarm of malicious UAVs. In general, even today there are no foolproof general authentication mechanisms, and even more so for networks involving swarms of drones.

Therefore, the purpose of this work is to conduct an analytical review and consider approaches to the creation of UAV/drones swarm authentication procedures with wireless equipment on board for the 5G NR network, taking into account the features of swarm formation and the requirements for 5G authentication.

The plan of the article is as follows. First, we consider the requirements of the current 3GPP recommendations for the possible services of drones in the 5G radio access network and for the authentication of individual drones in the 5G network. Next, we outline the requirements for the characteristics and features of the deployment and operation of a swarm of drones designed to connect to the 5G network. Finally, we present authentication methods and procedures that

could be used to connect a swarm of drones to a 5G network.

II. Regulatory requirements for drone authentication in the 5G NR network

Currently, a number of documents of the 3GPP organization already provide a certain technical foundation and recommendations for the use of individual drones with telecommunication equipment in the 5G network and can be useful in the implementation of such systems. In particular, documents TS 22.125 and TS 29.257 [13, 14] define the requirements for services for drones in the 5G network. It describes the characteristics that must be supported for the effective use of drones; technical report TR 38.889 [15] presents the results of research into the possibilities of using the 5G network in the unlicensed spectrum for communication with unmanned aerial vehicles; report TR 38.912 [16] describes the results of research on the integration of unmanned aerial vehicles (UAV) in the 5G NR network; document TR 38.811 [17] investigates the support of 5G NR networks in satellite systems, which may be important for communication with drones in remote areas.

The key features of the 3GPP architecture according to ETSI TS 123 256 for UAV integration with 5G NR are presented in Fig. 1 [18].

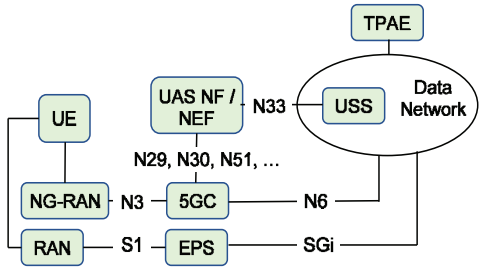

Fig. 1. System architecture 5GS and EPS for UAV:
5GC – 5G Core;
EPC – Evolved Packet System;
NEF - Network Exposure Function;
NG-RAN – Next Generation Radio Access Network;
RAN – Radio Access Network;
TPAE - Third Party Authorized Entity;
UAS NF - UAS Network Function;
UAS - Uncrewed Aerial System;
UAV - Uncrewed Aerial Vehicle;
UE – User Equipment;
USS - UAS Service Supplier

The following functions were established for the operation of the new architecture:

- USS (UAS Service Supplier) is an organization that supports the safe and efficient use of airspace by providing services to the operator/pilot of an unmanned aerial vehicle to meet the operational requirements of UTM (Uncrewed Aerial System Traffic Management);

- UAS NF (UAS Network Function) is a new 3GPP network function used for external access to USS services, including UAS authentication/authorization, UAS flight authorization, UAV-UAVC communication authorization (UAVC - UAV Controller), UAV tracking and control QoS and traffic filtering for communication, as well as to support remote identification;

- TPAE (Third Party Authorized Entity) is one of the components of the remote identification system, where it can control the UAV, access and track the UAV data, and control the UAV, canceling the UAVC if necessary. TPAE can be considered as UE, NF, or third party, depending on the application scenarios. It can be authorized by UTM to interact with UAV sets.

For UAV identification, the 3GPP organization introduced UAV remote identification at the CAA (Civil Aviation Administration) level. Such a UAV ID acts as a globally unique identification that is electronically and physically readable and tamper-proof, allowing the recipient to contact the correct USS for information about the UAV and can be assigned exclusively to the USS by means outside 3GPP or designated USS using the 3GPP system [19].

The first step for a UAV owner is to register the latter with USS outside of 3GPP through a procedure that can take place offline or via an Internet connection. During this procedure, the CAA-level UAV ID is configured in the UAV, and avionics-level information (such as UAV serial number, UAV operator information, etc.) is provided to the USS.

The UE on board the UAV then registers to the 3GPP network using existing 3GPP primary authentication procedures with MNO (Mobile Network Operator) credentials stored in its USIM (Universal Subscriber Identity Module).

After the UE is successfully authenticated, the initial UUAA (UAV USS Authentication and Authorization) procedure is performed to allow the 3GPP core network to verify that the UAV is successfully registered with the USS. In 5G, this procedure may occur during 3GPP registration or during PDU (Packet Data Unit) session establishment for UAS services.

The registration procedure has been specifically extended to allow the UE to specify its CAA-level UAV ID in the new Service-level-AA container included in the registration request message that initiates the AMF (Access and Mobility Management Function) and also in the installation request message session PDU triggering SMF (Session Management

Function) to initiate UUAA with USS via UAS NF [20].

Document TR 38.811 [17] describes the radio aspects of the use of unmanned aerial systems (UAS), including high-altitude aerial platforms (HAPS) as a base station. At the same time, a UAV with an on-board base station is designated as UxNB, and the latter can act not only as a base station, but also as a repeater.

In order for a UAV to be accepted as a UxNB, the following prerequisites must be met:

- the UAV must be equipped with on-board equipment that supports the base station function;
- The UAV can fly to a specified area independently or under the control of an operator, and then hover over this area for a certain period of time;
- UxNB is able to connect via a wireless connection to the 5G base network and work as its base station;
- before the UxNB is operational, it must be authorized by the 5G backbone network.

An example scenario of using UxNB can be as follows. The operator finds that some areas require temporary coverage, but such coverage cannot be achieved by installing a fixed base station. In this case, the use of UxNB is the most suitable and the scenario will be as follows:

1) the operator has decided that a certain area needs temporary coverage, which can be implemented by deploying UxNB;

2) all the necessary parameters for the implementation of this coverage are determined;

3) specific UxNBs are sent to a defined zone;

4) after arriving in the target area, each UxNB downloads the functions of its base station and receives authorization from the NMS (network management system);

5) NMS downloads configuration data to UxNB;

6) UxNB configures and transfers the functionality of its on-board base station to operational mode;

7) during operation, the UxNB does not move relative to the ground. A UE can access a 3GPP network through a single UxNB. The user does not feel the difference between the UxNB service and a regular stationary base station;

8) The UxNB turns off its base station functionality and returns home in the event that the end of temporary coverage support is approaching or due to insufficient power supply of the UxNB.

In principle, the actions of the 5G backbone network for drone authentication are very similar to those of the UE. Summarizing the existing provisions and schemes of drone authentication [21-23], the following stages can be distinguished:

1) the on-board processor of the drone calculates SUCI (subscription concealed identifier), encrypting SUPI (subscription permanent identifier) with the public key of the base station (BS);

2) the drone sends SUCI to the AMF function (access and mobility management function);

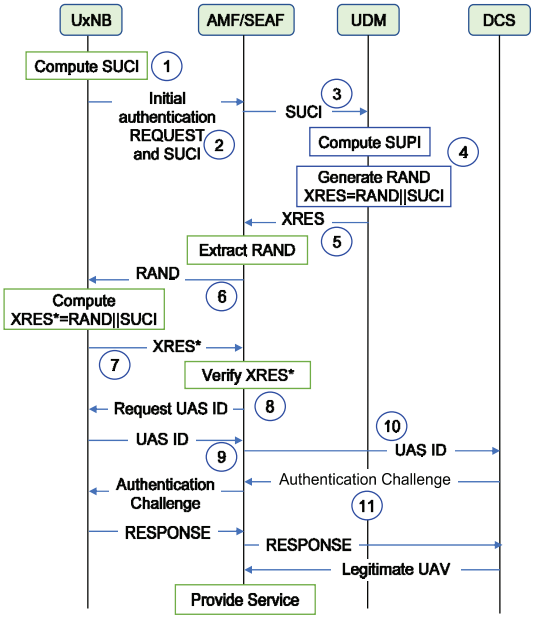

Fig. 2. Drone authentication according to the 3GPP Rel-17 (DCS – Drone Control Station)

3) AMF provides SUCI to UDM (unified data management);

4) UDM decodes the SUCI and compares the SUPI with the existing database; if SUPI is valid, then UDM generates a random value RAND and adds to the random value SUCI;

5) UDM sends back to AMF RAND and SUPI;

6) AMF extracts the RAND and transfers it to the drone;

7) the drone adds the SUCI to the random value and sends it back to the AMF;

8) if the AMF confirms the identity of the drone, the UAS ID is requested from the drone;

9) the drone sends the UAS ID to the AMF;

10) AMF sends the ID to the control station;

11) DCS and drone perform re-authentication; after receiving confirmation from DCS, AMF starts to provide 3GPP service for the drone on-board equipment.

III. Drone Group and Swarm Scenarios

As you can see, the standards for the 5G network provide us with a description and recommendations for

the authentication procedures of an individual drone (UE or UxNB). The problem arises when we want to connect not an individual drone, but a group or swarm of them. In the case of a group, the connection can happen sequentially with each member of the group, which of course increases the connection time and weakens the security of authentication. In this case, it is possible to use authentication approaches for a group of drones as for a group of IoT devices. But at the same time, for the UxNB mode, there will be a significant restriction on the traffic of a separate drone, as for a regular IoT device with a low bandwidth.

Of course, you need to understand that a group of drones is not a swarm of drones at all. A group of drones, or as they are called a fleet of drones, is a discrete association of completely independent UAVs to perform one common task. Management of members of such a group can be centralized or individual. In the latter case, the number of drones in the group cannot be large. In addition, communication between individual members of the group can take place centrally through the 5G backbone network. Therefore, a group of drones consists of separately authenticated independent members with different identifiers. And this means that the individual procedure described earlier is suitable for their authentication. The fewer drones there are in the group, the faster and more reliable the authentication of this group will be.

It is worth noting that a swarm of drones is not just a significant number of them. Swarm means primarily the autonomous interaction of drones between themselves or the queen/leader of the swarm and the same control when performing tasks [24, 25]. Perhaps the swarm could even have an internal autonomous distributed computing system for the operation of artificial intelligence. A swarm differs from a group in its isolated integrity and independence (self-organization) to fulfil the set goal.

The proposed constructions of some swarm management strategies: centralized and decentralized with a leader/host, collective self-management with information exchange, decentralized management with forecasting, self-organization without information exchange [26, 27].

The drone swarm is an evolving and evolving system: drones can join or leave the swarm. Thus, there must be a security mechanism to prevent the intrusion of an intruder drone. Moreover, the security system should be implemented in a distributed way to maintain the stability of the swarm [28]. There are times when identifiers and encryption keys can be distributed to escort ground stations during mission preparation, but this is not always possible, especially when separation of powers between swarm members must be maintained. In addition, care should be taken not to functionally overload any particular drone leader that could be detected by an attacker.

Thus, [21] describes the distributed structure of a swarm of drones, in which swarm members form three subgroups that have different powers/responsibilities. The first group that ensures the integrity of the swarm is the boundary drones, or guard drones, whose responsibility is to monitor the departure and joining of drones, as well as to identify new members in the swarm. The second group is represented by network drones that perform network operations and procedures in the swarm itself. The third group of drones provides services and is called service (service drones). Since the swarm has a dynamic structure, the number of drones in each of the groups can change depending on the needs of the swarm to perform the task assigned to it.

The most common management structure is leader-follower [29]. Here, one drone is the leader, which, using autopilot or remote control, determines the trajectory of the swarm and periodically transmits commands to the members of the swarm (its followers). Swarm members follow commands and perform tasks. Despite all the benefits and potential of drone swarms, maintaining communication within the swarm remains a challenge, especially when the swarm membership is constantly changing. To ensure communication with previous or future swarm members is secure, the encryption key must be instantly updated and synchronized between all swarm members.

So, as we can see, depending on the swarm management structure, a different method of authentication will be needed, which complicates the unification of such procedures for a swarm of drones. Authentication procedures for drone swarms in 5G can be implemented through the following approaches:

- individual authentication, when each drone as a swarm member undergoes authentication with one NR 5G ground station; you can consider such an approach as authentication of a group of IoT devices, if the traffic of the swarm is very limited;
- group authentication through a leader drone that communicates with swarm members and the 5G operator's network;
- group distributed authentication through boundary drones.

IV. Approaches to creating drone swarm authentication procedures

Group authentication through drone-leader. In this case, authentication is performed through the leader

drone with all members of the swarm. As an example, an authentication mechanism based on distributed delegation is proposed in [30] to reduce the service traffic directed to the 5G operator's core network. In this scheme, legitimate drones are authorized as proxy delegated signers to perform authentication on behalf of the underlying network. In addition, a mechanism for selecting and moving a new leader drone from/to an existing swarm is added.

Proximity Services (ProSe), which is a D2D (Device-to-Device) technology that allows devices to discover each other and communicate directly, provides the basis for interaction between drones. The security and privacy aspects of ProSe in 5G were defined in 3GPP Release 17 (TS 33.503) [31]. As shown in Fig. 3, UEs A, B, and C are 5G ProSe-enabled UEs that support 5G ProSe requirements and related procedures. The direct side link radio interface between UEs is called PC5. UEs A and B connect to the 5G Core (5GC) via the gNB using a 3GPP air interface called Uu. UE C, which is outside the network coverage area, acts as a remote UE and can receive a connection through another UE (such as UE B), which acts as a relay.

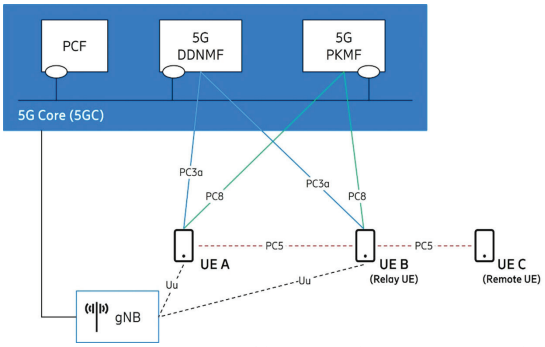

Fig. 3. Some components and interfaces for 5G ProSe security (source of the figure [31])

The policy control function (PCF) in the context of ProSe provides UEs (for example, UEs A, B and C in Fig. 3 above) with the necessary policies and parameters to use 5G ProSe services. The 5G direct discovery name management function (DDNMF) handles the network actions required for direct discovery (interacts with the UE through the PC3a interface). The 5G ProSe key management function (PKMF) interacts with the UE via the PC8 interface and handles the network operations required to manage the security keys to enable remote/relay detection and communication of the UE. The PC8 and PC3a interfaces rely on the 5GC user plane for transport (IP layer). It is clear that as a UE we can use swarm drones.

At the top level, 5G ProSe has three security functions: direct discovery security, direct communication security and relay communication security.

The standard ProSe procedure can take a long time when there are a large number of drones in a swarm. Therefore, for such a scenario, a so-called lightweight security model for drone authentication via 5G ProSe is proposed in [30], which minimizes the number of drone message exchanges with the 5G core network. In particular, authentication of the device based on the signature of the proxy server is introduced. The leader drone first broadcasts its unique proxy signature, and then other drones that should join the swarm respond with their proxy signature (Fig. 4). In all these authentication messages, the original signer is the underlying 5G network without the need to exchange messages after each new drone join/disconnect.

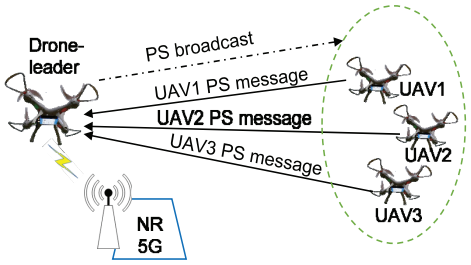

Fig. 4. Drone authentication message (PS - Proxy Signature)

An important component of such group authentication is the concept of proxy signature, a signature scheme in which the original signer delegates its signature capabilities to a proxy signer [32]. The proxy signer then creates a signature on behalf of that original signer. When a recipient verifies a proxy's signature, it verifies both the signature itself and the original signer's delegation. The basic methodology of proxy signing is that the originating signer first creates a signature on the delegation information (proxy signer ID or any warrant information) and secretly transmits it to the proxy signer. The proxy signer uses this signature as the proxy's private key or to generate the proxy's private key. Because the proxy key pair is generated from the original signer's signature in the delegation information, any verifier can verify the original signer's agreement against the proxy's signature.

Group distributed authentication through edge drones. Group distributed authentication scenarios offer more solutions than the drone leader authentication case. Here, a solution is possible for several cases at once, for example, authentication of

new drones (entering the swarm or leaving the swarm) and merging two separate drone swarms.

The cause of latency issues in 5G NR is the authentication request from each new party (individual drone or swarms). If the number of new members is too large, the servers in the core network may experience a delay or failure altogether.

Security drones, as shown in Fig. 5, can perform group authentication with new parties and solve the latency problem by authenticating more than one drone at the same time.

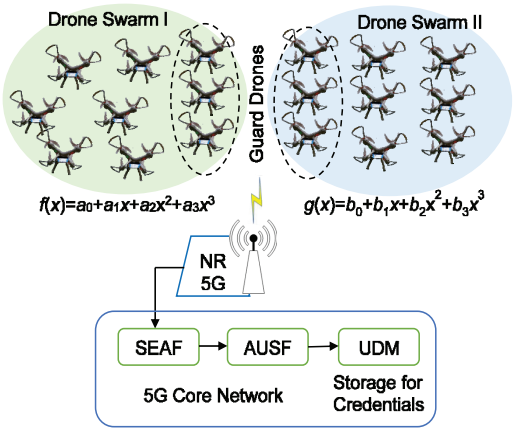

Fig. 5. Combining two swarms of drones (UDM - Unified Data Management, AUSF - Authentication Security Function, SEAF - Security Anchor Function)

In addition to adding a new drone to a swarm of drones, there may be a need to merge two swarms. Each drone swarm uses a different private key polynomial (f(x); g(x)) for group authentication, as shown in Fig. 5 [21, 23]. Polynomials are known only to the underlying network. Each drone in the swarms has only public and private keys, which are (xdrone; f(xdrone) P) and (f(xdrone)) for swarm I and (xdrone; g(xdrone) P) and (g(xdrone) P))) for swarm II.

The steps of such a scenario are as follows [21]. The guard drone identified by the guard drones in the two swarms requests private and public key pairs from the core network for the opposite group. The core network shares the valid keys with the corresponding security drone by encrypting the keys with the private key of the security drone. The guard drone shares public key pairs with the opposing swarm after the keys are decrypted. Guard drones in the opposing group's swarm send their public key pairs to each other. As each drone in the opposing swarm receives a valid public key equal to the threshold value, it performs group authentication.

If group authentication is valid, the group key of the second swarm is encrypted and sent to the sharing drone in the first swarm. The security drone in the first swarm encrypts the second swarm's key with the first swarm's key and sends it to all swarm members. After this stage, the two swarms are merged, and the group key of the second swarm is used in intragroup communication.

An example of two swarms of drones confirming each other is shown in Fig. 6. In this example, the threshold value is four, and three drones are guard drones of the second swarm, and one drone is a guard drone selected from the first swarm. The algorithm in Fig. 6 can be used by two swarms to authenticate each other and determine the swarm key for the newly created swarm.

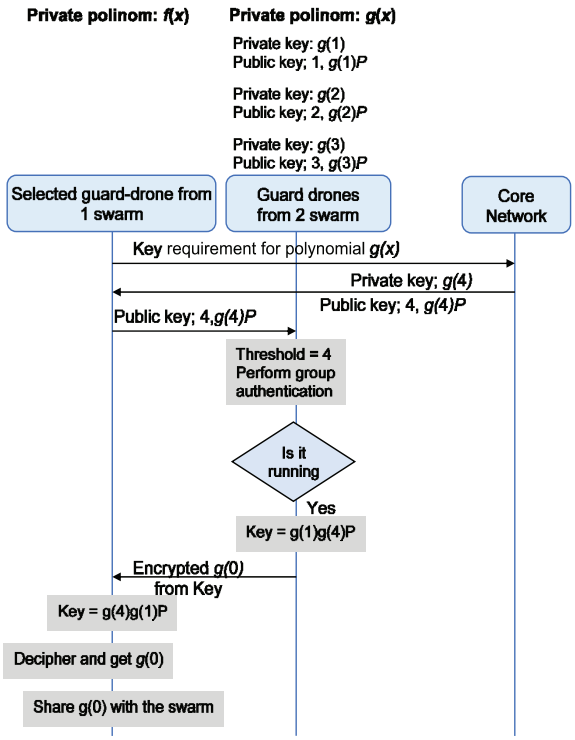

Fig. 6. Authentication of two swarms of drones. When the threshold value of 4 is selected for the scheme, one drone from the first swarm and three security drones from the second swarm are sufficient for group authentication

V. Conclusion

The widespread use of small UAVs, as well as the large expansion of wireless 5G networks, require new security measures to prevent unauthorized access to sensitive data.

Identification and Authentication for a mobile operator's network using drones allows for secure communication between its main components. This makes it possible to recognize the very drones that participate in the formation of such a network. Drone

authentication often protects the communication channel by preventing replay attacks. The development of drone radio access control mechanisms, such as authorization and authentication mechanisms, remain relevant researches for the construction of promising radio access networks involving UAVs.

When working with a swarm of drones, in addition to the usual problems with encryption and authentication (within the swarm and for communication between the swarm and the ground control station), there are additional problems related to the constant change in the composition of the swarm and its hovering position: drones can join or leave a swarm.

Currently, a number of recommendations of the 3GPP organization provide certain technical provisions and recommendations for the use of individual drones with wireless equipment in the 5G network and can be useful in the implementation of such systems. For example, according to ETSI TS 123 256, the key functions of the 3GPP architecture for the integration of UAVs with 5G NR have been developed. The following functions were established for the operation of such an architecture: USS, UAS NF and TPAE. The actions of the 5G backbone network for drone authentication are very similar to those of the UE.

Depending on the swarm management structure, a different method of authentication will be needed, which makes it difficult to unify such procedures for a swarm of drones. Authentication procedures for a swarm of drones in 5G can be implemented through the following approaches: individual authentication, when each drone as a member of the swarm undergoes authentication with one NR 5G ground station; you can consider such an approach as authentication of a group of IoT devices, if the traffic of the swarm is very limited; group authentication through a leader drone that communicates with swarm members and the 5G operator's network; group distributed authentication through edge drones.

Group authentication via a drone leader is presented, where authentication is performed through a mechanism based on distributed delegation to reduce the service traffic directed to the 5G operator's core network. Here, legitimate drones are authorized as proxy delegated signers to perform authentication on behalf of the underlying network.

Group distributed authentication through boundary drones is considered, which offers more solutions than the case of authentication through a leader drone. Here, a solution is possible for several cases at once, for example, authentication of new drones (entering the swarm or leaving the swarm) and merging two separate drone swarms.

It has been confirmed that the introduction of special group procedures for the authentication of a swarm of drones in the 5G network can significantly improve the quality of the provision of telecommunication services.

REFERENCES

1. M. A. Khan, N. Kumar, S. A. H. Mohsan, W. U. Khan, M. M. Nasralla, M. H. Alsharif, J. Zywiołek, I. Ullah, “Swarm of UAVs for Network Management in 6G: A Technical Review”, IEEE Transactions on Network and Service Management, 20 (1), pp. 741-761 (2023), http://dx.doi.org/10.1109/TNSM.2022.3213370.

2. S. Ahmadi, 5G NR: Architecture, Technology, Implementation, and Operation of 3GPP New Radio Standards. - London: Academic Press, 2019. – 1020 p.

3. B. Li, Z. Fei, Y. Zhang, “UAV Communications for 5G and Beyond: Recent Advances and Future Trends”, IEEE Internet of Things Journal, Vol. 6, Issue 2, pp. 2241 – 2263. (2019), https://doi.org/10.1109/JIOT.2018.2887086.

4. M. Ilchenko, S. Kravchuk, “Mobile infocommunication systems”, Information and Telecommunication Sciences, Vol. 11, Number 1, pp. 11-19 (2020), https://doi.org/10.20535/2411-2976.12020.11-19.

5. S. O. Kravchuk, Theory of mobile information communication systems. System architecture [Electronic resource] / S. O. Kravchuk. – Electronic text data (1 file: 18.17 MB). – Kyiv: Igor Sikorsky KPI, 2023. – 683 p. Retrieved from https://ela.kpi.ua/handle/123456789/53198.

6. 3GPP TS 29.255 V18.2.0 (2023-12). Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Uncrewed Aerial System Service Supplier (USS) Services; Stage 3 (Release 18), 29 p., https://portal.3gpp.org.

7. 3GPP TS 29.256 V18.3.0 (2023-12). Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; 5G System; Uncrewed Aerial Systems Network Function (UAS-NF); Aerial Management Services; Stage 3 (Release 18), 28 p., https://portal.3gpp.org.

8. M. M. Kaidenko, S. O. Kravchuk, “Anti-Jamming System for Small Unmanned Aerial Vehicles”, 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD), 19-21 Oct. 2021, Kyiv, Ukraine, pp. 1-4, DOI: 10.1109/APUAVD53804.2021.9615403, Date Added to IEEE Xplore: 26 November 2021.

9. M. Kaidenko, S. Kravchuk, “Protection against the effect of different classes of attacks on UAV control channels”, Information and Telecommunication Sciences, No. 1 (2022), pp. 35-43, DOI: https://doi.org/10.20535/2411-2976.12022.35-43.

10. S. Kravchuk, I. Kravchuk, “Wireless Connection of Drones to the Base Station of the Existing Terrestrial Mobile Network”, in: Ilchenko, M., Uryvsky, L., Globa, L. (eds) Progress in Advanced Information and Communication Technology and Systems. MCiT 2021. Lecture Notes in Networks and Systems, vol 548. Springer, Cham. (ISSN2367-3370, E-ISSN2367-3389, ISBN 978-3-031-16367-8) – pp. 377–397 (2023), https://doi.org/10.1007/978-3-031-16368-5_19.

11. S. Kravchuk, L. Afanasieva, “Three-Dimensional Model of the Radio Links Formation between the Base Station Antenna and the User Terminal with Retransmission through the Unmanned Aerial Vehicle”, 2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 29 Nov.-3 Dec. 2021, Odesa, Ukraine, pp. 93-96, https://doi.org/10.1109/UkrMiCo52950.2021.9716589 (https://ieeexplore.ieee.org/abstract/document/9716589).

12. UAV Networks and Communications, Edited by K. Namuduri, S. Chaumette, J. H. Kim, J. P. G. Sterbenz, Cambridge University Press, 2018, ISBN 978-1-107-11530-9.

13. 3GPP TS 22.125 V19.1.0 (2023-12). Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Uncrewed Aerial System (UAS) support in 3GPP; Stage 1 (Release 19), 17 p., https://portal.3gpp.org.

14. 3GPP TS 29.257 V18.3.0 (2024-03). Technical Specification. 3rd Generation Partnership Project; Technical Specification Group Core

Network and Terminals; Application layer support for Uncrewed Aerial System (UAS); UAS Application Enabler (UAE) Server Services; Stage 3 (Release 18), 158 p., https://portal.3gpp.org.

15. 3GPP TR 38.889 V16.0.0 (2018-12). Technical Report. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on NR-based access to unlicensed spectrum (Release 16), 119 p., https://portal.3gpp.org.

16. ETSI TR 138 912 V14.1.0 (2017-10). 3GPP TR 38.912 version 14.1.0 (Release 14). 5G; Study on new radio access technology. 77 p., http://www.etsi.org/standards-search.

17. 3GPP TR 38.811 V15.4.0 (2020-09). Technical Report. 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Study on New Radio (NR) to support non-terrestrial networks (Release 15), 127 p., https://portal.3gpp.org.

18. ETSI TS 123 256 V17.3.0 (2022-07) 5G; Support of Unscrewed Aerial Systems (UAS) connectivity, identification and tracking; Stage 2 (3GPP TS 23.256 version 17.3.0 Release 17), http://www.etsi.org/standards-search.

19. S.O. Kravchuk, "Drone ID open architecture and remote drone identification protocol", Proceedings of the International Scientific Conference "Moden Challenges in Telecommunications", April 18-21, 2023, Kyiv, Ukraine, pp. 189–191 (2023). Retrieved from http://conferenc.its.kpi.ua/proc/article/view/281720.

20. L. Chaponniere, "TSG CT work on UAS Connectivity, Identification and Tracking, 3GPP Technologies" (2022), https://www.3gpp.org/technologies/tsg-ct-work-on-uas-connectivity-identification-and-tracking.

21. Y. Aydin, G. K. Kurt, E. Ozdemir, H. Yanikomeroglu, "Group Authentication for Drone Swarms", 2021 IEEE International Conference on Wireless for Space and Extreme Environments (WiSEE), Cleveland, OH, USA, 12-14 October (2021) pp. 72-77. https://doi.org/10.1109/WiSEE50203.2021.9613831.

22. 3GPP TR 33.854 V17.1.0 (2021-12). Technical Report. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on security aspects of Uncrewed Aerial Systems (UAS) (Release 17). 62 p., https://www.3gpp.org.

23. Y. Aydin, G. K. Kurt, E. Ozdemir, H. Yanikomeroglu, "Authentication and Handover Challenges and Methods for Drone Swarms", IEEE Journal of Radio Frequency Identification, Vol. 6, pp. 220 - 228 (2022), https://doi.org/10.1109/JRFID.2022.3158392.

24. X. Chen, J. Tang, S. Lao, "Review of Unmanned Aerial Vehicle Swarm Communication Architectures and Routing Protocols", Appl. Sci. 10, 3661 (2020), doi:10.3390/app10103661.

25. T. Zeng, M. Mozaffari, O. Semiari, W. Saad, M. Bennis, M. Debbah, "Wireless Communications and Control for Swarms of Cellular-Connected UAVs", 52nd Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, (2018), pp. 719-723. doi: 10.1109/ACSSC.2018.8645472

26. S. Kravchuk, L. Afanasieva, "Formation of a wireless communication system based on a swarm of unmanned aerial vehicles", Information and Telecommunication Sciences, No 1, pp.11-18 (2019), DOI: https://doi.org/10.20535/2411-2976.12019.11-18

27. S.O. Kravchuk, I.M. Kravchuk, "Using RFID technology at operating a drone swarms in communication system mode", Information and Telecommunication Sciences, Vol. 11, N. 2 (21), pp. 16-23 (2020), https://doi.org/10.20535/2411-2976.22020.16-23.

28. UAV Networks and Communications, Edited by K. Namuduri, S. Chaumette, J. H. Kim, J.P.G. Sterbenz, Cambridge University Press, 2018, ISBN 978-1-107-11530-9

29. Z. Liu, X. Yu, C. Yuan, Y. Zhang, "Leader-follower formation control of unmanned aerial vehicles with fault tolerant and collision avoidance capabilities," 2015 International Conference on Unmanned Aircraft Systems (ICUAS) 09-12 June (2015), https://doi.org/10.1109/ICUAS.2015.7152392

30. M. A. Abdel-Malek, K. Akkaya, A. Bhuyan, A. S. Ibrahim, "A Proxy Signature-Based Swarm Drone Authentication with Leader Selection in 5G Networks", IEEE Access, Vol, 10, pp. 57485-57498 (2022). DOI: 10.1109/ACCESS.2022.3178121

31. M. Wifvesson, P. K. Nakarmi, 5G Release 17: Overview of new RAN security features, Ericsson Blog (2022), https://www.ericsson.com/en/blog/2022/10/3gpp-release-17-security-ran

32. B. Lee, H. Kim, K. Kim,''Strong proxy signature and its applications'', in Proc. SCIS 2001, The 2001 Symposium on Cryptography and Information Security, Oiso, Japan, January 23-26, 2001 The Institute of Electronics, Information and Communication Engineers, pp. 603–608 (2001).

Кравчук С.О., Кравчук І.М.

Аутентифікація безпроводових систем на базі рою дронів як складової частини архітектури мережі радіодоступу 5G

Проблематика. Встановлюючи заходи безпеки для телекомунікаційних мереж із задіянням безпілотних літаючих апаратів (БПЛА), слід враховувати такі характеристики, як висока масштабованість, різноманітність пристроїв і висока мобільність. Автентифікація є фундаментальною властивістю, яка дозволяє мережі із БПЛА встановлювати безпечний зв'язок між її основними компонентами. Автентифікація також захищає мережу БПЛА від зловмисників, які видають себе за законні БПЛА. Аутентифікація БПЛА може додатково захистити канал зв'язку, запобігаючи уособленню та повторним атакам. Розробка схем контролю доступу БПЛА, таких як механізми авторизації та автентифікації, залишається складною проблемою для дослідження в мережах БПЛА. Ще більше ускладняються функціонування мережі, коли вона взаємодіє із множиною БПЛА, яка називається роєм. Рій за своєю природою має динамічну структуру, і це піднімає проблему ненадійних обмежень на БПЛА в його складі. Відоме стандартизоване рішення для аутентифікації одного дрона з використанням нової 5G радіомережі (NR), але для рою дронів – це відкрите поле досліджень. Спільне використання ключів автентифікації для кожного БПЛА, як описано в 5G NR, не масштабується для груп БПЛА.

Мета досліджень. Метою даної роботи є проведення аналітичного огляду та розгляду підходів до створення процедур автентифікації рою БПЛА/дронів з безпроводовим обладнанням на борту до мережі 5G NR з урахуванням особливостей формування рою та самих вимог на автентифікацію 5G.

Методика реалізації. Аналіз факторів, що впливають на якість надання телекомунікаційних послуг із задіянням БПЛА у мережах п'ятого покоління. Аналіз відомих публікацій, присвячених впровадженню мереж 5G та задіяння в них дронів. Проведення порівняння реалізації процедур аутентифікації БПЛА із бортовим безпроводовим обладнанням у мережі 5G.

Результати досліджень. Широке використання малих БПЛА, а також велике розширення безпроводового підключення мереж 5G, вимагають нових заходів безпеки для запобігання несанкціонованому доступу до конфіденційних даних.

Ідентифікація та Authentication для мережі оператора мобільного зв'язку із застосуванням дронів дозволяють встановлювати безпечний зв'язок між її основними компонентами. Це дозволяє розпізнавати самі дрони, які беруть участь у формуванні такої мережі. Аутентифікація дрону часто захищає канал зв'язку шляхом запобігання повторних атак. Розробка механізмів контролю радіодоступу дрону, таких як механізми авторизації та автентифікації, залишаються актуальними дослідженнями для побудови перспективних мереж радіодоступу із задіянням БПЛА.

Підтверджено, що введення спеціальних групових процедур аутентифікації рою дронів у мережі 5G можуть значно покращити якість надання телекомунікаційних послуг.

Висновки. При роботі з роєм дронів до звичайних проблем із шифруванням та автентифікацією (всередині рою та для зв'язку між роєм та наземною станцією контролю), мають місце і додаткові проблеми, пов'язані із постійною зміною складу рою і положенню його зависання: дрони можуть приєднуватися або залишати рій.

В залежності від структури управління роєм знадобиться різний спосіб аутентифікації, що ускладнює уніфікацію таких процедур для рою дронів. Процедури аутентифікації для рою дронів в 5G можуть бути реалізовані за рахунок наступних підходів: індивідуальної аутентифікації, коли кожен дрон як член рою проходить аутентифікацію з однією наземною станцією NR 5G; можна розглядати такий підхід як аутентифікація групи приладів IoT, якщо трафік рою дуже обмежений; групової аутентифікації через дрона-лідера, який має зв'язок з членами рою та мережею оператора 5G; групової розподіленої аутентифікації через граничні дрони.

Представлено групову аутентифікації через дрон-лідер, де аутентифікація проводиться через механізм на основі розподіленого делегування для зменшення службового трафіку, що направлений до базової мережі оператора 5G. Тут легітимні дрони авторизовані як проксі-делеговані підписувачі для виконання автентифікації від імені базової мережі.

Розглянуто групову розподілену аутентифікацію через граничні дрони, що пропонує більше рішень ніж для випадку аутентифікації через дрон-лідер. Тут можливе рішення одразу для декількох випадків, наприклад, автентифікація нових дронів (входять до рою або виходять з рою) і об'єднання двох окремих роїв дронів.

Ключові слова: *5G; NR 5G; безпека; аутентифікація; групова аутентифікація; ідентифікація; дрон; БПЛА; рій дронів.*