The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No.4 (2024)

DOI: 10.62524/msj.2024.2.4.18

Problems of Organizing Communication and Controlling Swarms of Unmanned Aerial Vehicles (drones)

Serhii Tarapovskyi
Head of Research Department
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: tarapovskyi@gmail.com
ORCID: 0009-0004-4951-6056

Mykhailo Antonishyn
Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: antonishin.mihail@gmail.com
ORCID: 0000-0002-2665-0066

Oleksii Hramak
Leading Research Fellow
The Central Research Institute of the Armed Forces of Ukraine
03049, Povitrianykh Syl avenue, 28 B, Kyiv, Ukraine
e-mail: Hramakoleksij@gmail.com
ORCID: 0009-0008-5603-9779

Roman Voitsekhovskyi
Adjunct of the Military Management Department of the State Military Management Institute
National Defence University of Ukraine
03049, Povitrianykh syl avenue, 28, Kyiv, Ukraine
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Oleh Tarasov
Candidate of Military Sciences, Associate Professor
Associate Professor of the Military Training Department
National Aviation University
03058, Lubomyr Huzar Avenue, 1, Kyiv, Ukraine
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

Abstract. The article explores important aspects of organizing communication and controlling swarms of unmanned aerial vehicles (drones). The authors examine the problems associated with solving the tasks of ensuring uninterrupted communication during the combat use of drones, coordinating their actions in the performance of tasks in real time. The article analyzes various approaches towards resolving these issues and provides recommendations for improving the efficiency of drone swarm management. The experience of using unmanned aerial vehicles during Russia's full-scale invasion of Ukraine has shown that there is a constant need to introduce new

approaches of using drones, including the use of swarms, which will significantly increase the effectiveness of inflicting fire damage on the enemy. Specifically for drone swarms, coordination and coherence in the process of their use is critical. Depending on how drone swarms are used in the control system, there are three main approaches to control them: single machine control, centralized control, and distributed control. To ensure continuous control of drone swarms, it is necessary to ensure the stability and security of drone swarm control channels. This is achieved by various data transmission protocols, communication channel standards, and data encryption.

Keywords: UAV, drones, unmanned systems, communication systems, control systems, unmanned complexes, control standards, SUAV, LoRa, LoRaWAN, IEEE 802.11s standard, SUCOM module.

Introduction

"Swarm warfare" is a method of using unmanned aerial vehicles (hereinafter referred to as drones) in combat operations as part of organized groups (swarms) of drones under a single plan to achieve a common goal. There are different approaches to organizing the control of drone swarms. Drones can be used individually under different control, controlled from one central point, or networked for autonomous operation. The materials [1]-[3] deal with the topical issue related to the creation and use of military drone swarms.

The world is increasingly moving from the individual use of drones to their organization into controlled groups of mass use - drone swarms - mobile autonomous unmanned aerial vehicles (air, ground, underwater or above-water) programmed to perform specific tasks. The current state of creation and prospects for the use of drone swarms, in particular for military purposes, in the leading countries indicate that with the development of artificial intelligence, advanced weapons systems and the latest materials, drone swarms may become dominant on the battlefield in the next 10-15 years. An example of the use of drones with single machine control is the Houthis' raid on a Saudi oil refinery in March 2021 with the help of 12 drones and centralized control is the organization by Syrian opposition forces in January 2018 of an attack by 13 drones on the Khmeimim air base and the Tartus logistics base of the Russian army in Syria.

WestPoint has been researching the use of drone swarms for a long time and closely. Their materials [4] examine the potential of drone swarm technology - the ability of drones to make autonomous decisions based on shared information. This technology can revolutionize the dynamics of conflicts, particularly in the field of national security. Drone swarms can be used to conduct search (reconnaissance) operations, detect and destroy enemy missiles in the process of performing air defense tasks and providing air cover for troops (forces) in operations (combat actions), and can be used as a new type of warfare as part of the defense forces. To achieve the full potential of drone swarms, it is necessary to develop capabilities in four key aspects: swarm size, diversity, individual customization, and ensuring the stability of data exchange channels. A publication by the DefenceBribge portal [5] notes that a swarm can autonomously coordinate large groups of drones using their artificial intelligence and ability to perceive the environment. They work together to perform common tasks and respond quickly and accurately to changes in their environment. This technology can be used in both military and civilian fields, including fighting forest fires and searching for missing people.

Materials and Methods

The article [6] proposes a method of maintaining drone swarms that will allow achieving high efficiency in performing certain tasks. Based on the characteristics of drone swarms, such as low cost, high integrity, and quite frequent information exchange, it combines the method of assessing the reliability of a multi-level complex network with the group maintenance method. Considering

the cost of grouping maintenance, the failure mechanisms of drones in different modes, and the impact of maintenance on the system, the authors optimize the grouping maintenance strategy using multi-objective planning for system cost and reliability. Compared to existing just-in-time maintenance methods, this method can significantly reduce the total cost of swarm maintenance while ensuring high sustainability of swarm missions. The results confirm its feasibility and effectiveness. To illustrate the method, a universal drone swarm mission scenario is used. This is schematically illustrated in the three-level model shown in Figure 1.

Another method considered in [7] is the proposed blockchain-based cross-domain authentication scheme (BCDAIoD). This method uses a chain with a multi-chain architecture, which allows for efficient querying and updating of different types of data. In the process of cross-domain authentication, drones can form groups to reduce the load on domain management nodes. In addition, BCDAIoD uses the mechanism of data exchange between domains to plan the combat operation of drones in advance, which further increases the efficiency of their use. Experimental results have shown that the cross-domain authentication time and computational cost of BCDAIoD are significantly lower than existing methods for maintaining many drones, as shown in Figure 2.

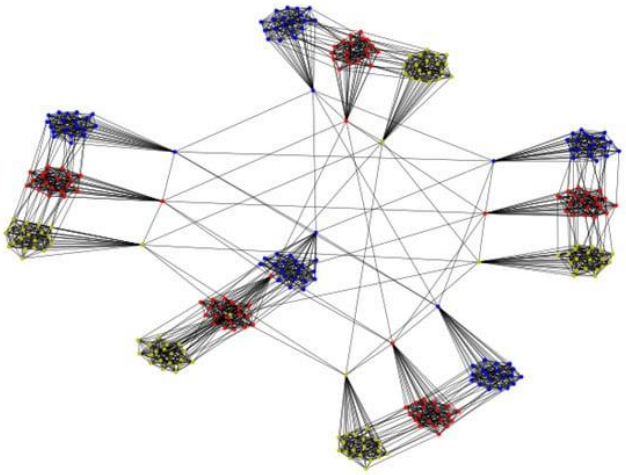

Figure 1. Three-level integrated network model

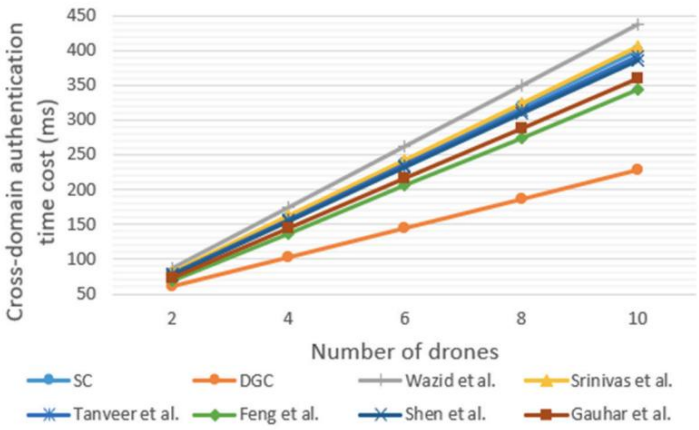

Figure 2. Cross-domain authentication time and computing costs

The authors of the article [8] propose an efficient method for planning a route for several drones that have to perform tasks in different regions. The method divides the solution process into two stages. First, considering the flight speed and the width of the scanning area, the authors

propose a new scheme for allocating regions based on the minimum resource consumption. This scheme determines the distribution of tasks and preliminary planning of drone routes. Second, given the trajectories of the drones, they are optimized based on a dynamic algorithm to reduce the transition time between regions. Numerical experiments have confirmed the effectiveness of the proposed method: the task execution time for homogeneous and heterogeneous (different types) drones has decreased by 5.1% and 3%, respectively, compared to the improved algorithm.

Materials in [9] propose an effective threat assessment model and a hierarchical scheme for assigning tasks to drone swarms in large-scale group interception scenarios. This work solves the problem of assigning tasks to multi-drones in large-scale group intercepts. The model takes into account drone-specific dynamic constraints and accurately describes the overall performance of a multi-drone joint intercept. The hierarchical scheme uses a network flow algorithm to optimize drone swarm configurations and/or prioritize targets. The results of simulations of the use of drone swarms confirm the feasibility and effectiveness of the proposed hierarchical scheme for assigning tasks to drone swarms.

Materials in [11] propose a hybrid communication architecture for swarms of unmanned aerial vehicles (drones) that uses heterogeneous radio network protocols based on communication protocols of the IEEE 802.11s data transmission standard, such as: LoRa and LoRaWAN. The article discusses the advantages, constraints, and possible implementation in relevant use cases.

Table 1. Data exchange protocols and frequencies at which they operate

Protocols	Frequencies
LoRa та LoRaWAN	433 MHz, 868 MHz and 915 MHz
SUCOM	LTE (900 MHz, 1800 MHz and 2600 MHz)

Materials [12] consider an intelligent cluster communication system for drone swarms in search and rescue missions. The ICBM-UAV protocol uses clustering to conserve drone battery power and optimize computation. This work revealed the advantages of ICBM-UAV over existing protocols such as AODV, OSLR in terms of data link capacity, and PDR protocol in terms of stable signal reception area given the existence of obstacles.

Data transmission channels of drone swarms are divided into two types:

• State Channels, which transmit information about the status of drones, such as coordinates, speed, altitude, battery power, and other parameters. This helps to avoid collisions and coordinate the actions of drones.

• Task Channels, which transmit data about the tasks that drones perform. For example, if one drone finds an object for delivery, it can notify other drones so that they don't waste time searching for it.

Information in both types of communication channels is transmitted wirelessly. High-intensity countermeasures can lead to deterioration or even loss of communication between the control center and the “drone swarm”.

Encryption mechanisms for data exchange in communication channels are an important part of ensuring its confidentiality and protection. The use of cryptographic methods, such as encryption and decryption, helps to ensure the security of information exchange in a drone swarm.

The most used encryption methods are:

- Hierarchical identity-based encryption. This method uses hierarchical identifiers to encrypt messages. Each drone has its own identifier and using this mechanism, they can exchange encrypted messages.

- Pseudonyms. Pseudonyms can be used for anonymous data exchange. Each drone can use a pseudonym to encrypt and decrypt messages without revealing its true identity.

- Cryptographic protocols. The use of cryptographic protocols, such as public key, hash

functions, and symmetric encryption, helps to ensure data confidentiality and authentication [13]-[17].

Table 2. Control protocols

№	Protocol Name	Brief description	Disadvantages
1	ICBM-UAV	ICBM-UAV allows the military to effectively use drones for reconnaissance, monitoring and defense.	ICBM-UAV is used only on high-altitude drones that can operate at altitudes above 9000 meters.
2	SBUS	SBUS is a serial protocol that transmits signals from a radio transmitter to a receiver. It allows many channels of information to be transmitted over a single channel.	1. Mono channel: SBUS transmits all channels through a single serial channel, which can lead to failures in the event of interference or interference. 2. Complexity of setup: To use SBUS, you need to configure signal converters, which can be difficult for beginners. 3. Limited number of channels: Although SBUS transmits many channels, the maximum number is limited to 16.
3	DSMX	These protocols are used in Spektrum radio systems. DSMX can automatically switch to a new frequency channel in case of signal loss.	1. The DSMX has 23 channels, which allows it to switch between them. This ensures less chance of interference. 2. Dynamic frequency mode: The DSMX can automatically switch between frequencies, which helps to avoid interference.
4	DSM2		1. Number of channels: The DSM2 has only 2 channels, which limits the control options. 2. Interference susceptibility: Due to the limited number of channels, the DSM2 may suffer from interference with other devices.
5	FPort	FPort is a combined protocol that combines SBUS and SmartPort. It allows the transmission of signals and telemetry simultaneously.	FPort is a protocol that currently still comes out of the SmartPort (S.Port) pin on the receiver, and this pin is usually inverted.
6	PPM	PPM (Pulse Position Modulation) and PWM (Pulse Width Modulation) are analog protocols used to transmit signals from a radio transmitter to a receiver.	1. Sensitivity to noise: if the pulses are offset, signal distortion may occur. 2. Limited accuracy: The pulse position is measured relative to a reference point, which can limit the accuracy of the transmission.
7	PWM		1. Power Loss: Turning the unit off and on may result in power loss. 2. Electromagnetic noise: fast switching may generate electromagnetic noise.
8	MAVLINK	MAVLINK is an open protocol for communication between drones and ground stations. It is used to transmit telemetry, commands, and drone status.	1. Power Loss: Turning the power supply off and on may result in power loss. 2. Electromagnetic noise: Fast switching may generate electromagnetic noise.
9	SmartPort	The SmartPort protocol allows telemetry data to be transmitted between the drone and the remote control, providing important information about the drone's status.	1. Security: If the protocol does not provide an adequate level of data protection, it can lead to the leakage of sensitive information. 2. Compatibility: If SmartPortal does not support standard protocols or is not compatible with other systems, it may limit its use. 3. Performance: If a protocol has a low data rate or high latency, it can affect system performance.

Results

Based on the materials of the above studies, it is proposed to apply three main methods of controlling drone swarms - single machine control, centralized control, and distributed control, schematically illustrated in Figure 5.

Single machine control is the remote control of a set of drones from separate control points, while they cannot exchange data with each other.

Centrated control is the control of drone swarms, which involves the transmission of commands to groups of drones in a unified manner. The distribution of responsibilities and interaction between drones, as well as the response to the situation on the battlefield, are carried out by sending instructions from the control center. The drones are connected to the control center via a single network, but they are not interconnected. This method is simple to implement, but the degree of intelligence during the autonomous interaction of UAVs is limited. As soon as the data link between the swarm and the control point is disrupted or the control point is destroyed, the swarm of drones in the air is out of control.

Distributed control is the control of swarms of drones, which involves connecting to a common network through data channels and using a cluster approach to exchange information and interact between drones in the "swarm". Control is performed without direct intervention, enabling the swarm of drones to achieve autonomous combat capabilities. This type of decentralized network, which does not require access points, is highly reliable and can continue to operate independently of ground communications. Even if a part of the UAV is lost, the network can be reconstructed without affecting the effectiveness of the swarm's operations.

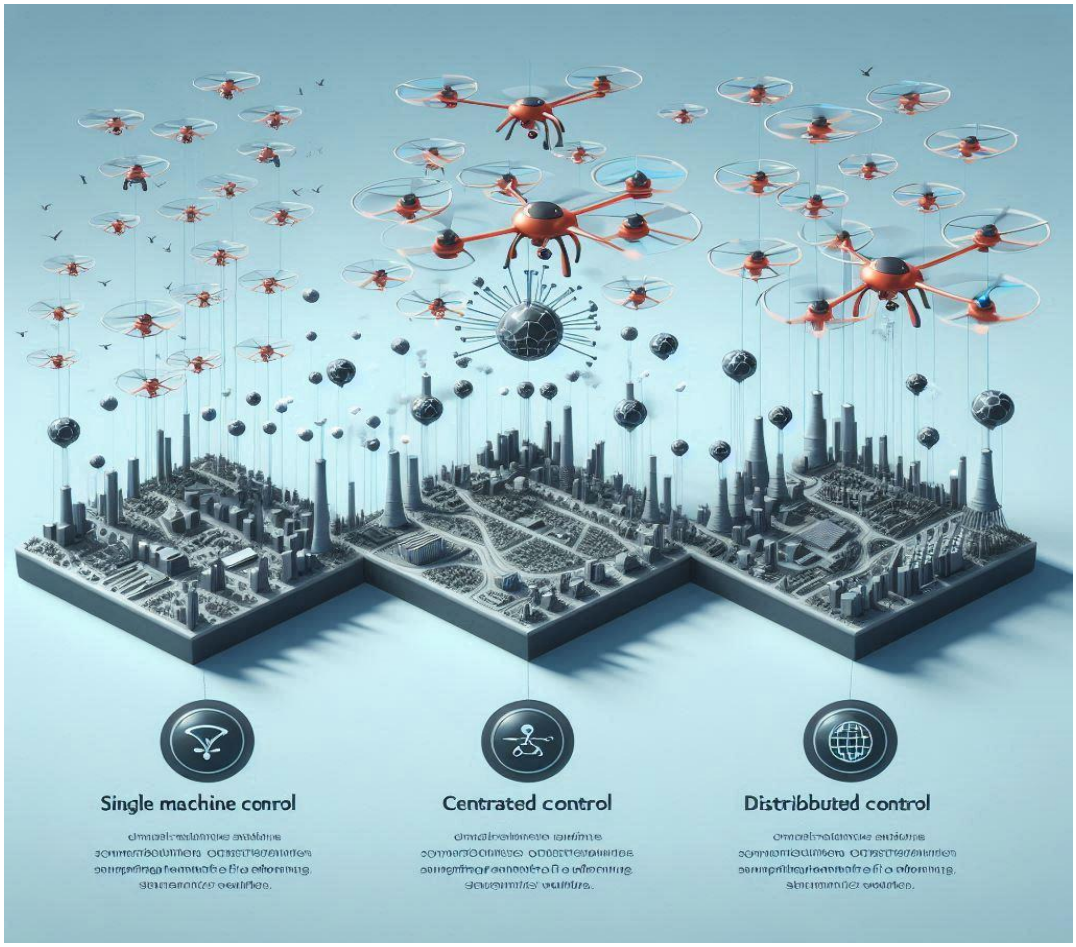

Figure 5. Methods of controlling drone swarms

The communication system uses protocols of the IEEE 802.11s data transmission standard to control drone swarms:

- LoRa is a long-range wireless technology that allows data to be transmitted over long distances (up to 10 km) using broadband modulated radio communications.
- LoRaWAN is a network protocol based on LoRa technology that allows low-power devices to communicate over long distances. A "star-to-star" topology is used to connect end devices with gateways.
- To increase the range of a drone swarm, an additional module based on the SUCOM protocol can be used, which can be installed on any drone and provides a drone control range of up to 40 km.

Discussions

With the development of localization, navigation, and communication technologies, drone swarms will operate autonomously, sharing responsibilities and coordinating their actions. It is important to solve open problems, such as controlling the autonomous management of drone swarms. For a drone swarm management system to function sustainably, it is necessary to counter adversary electronic warfare (EW). Several methods can be used to counter electronic warfare (EW) to maintain the functionality and security of drone swarm management.

Let's look at some of the key methods and technologies for countering EW.

1. The use of secure communication channels, which are encrypted using strong encryption algorithms such as AES-256 or ChaCha20 to protect data and control commands.

2. Frequency manipulation to protect against interception and jamming of signals using methods such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). These methods provide a constant change in transmission frequencies, which makes it difficult to attack the communication channel.

3. Redundancy and communication recovery due to multi-level channel duplication, which is carried out by using several independent communication channels (for example, Wi-Fi, mobile networks, specialized radio channels) for backup information exchange in case of suppression of the main channel.

4. Autonomous actions due to the provision of autonomous behavior algorithms that allow drones to perform tasks or safely return to the base in case of loss of communication.

5. Adaptive algorithms and artificial intelligence.

Adaptive routing algorithms - the use of algorithms that can dynamically change routes and communication methods depending on current conditions and detection of obstacles.

Artificial intelligence and machine learning - the use of artificial intelligence to analyze and predict EW attacks, as well as to adapt to new types of threats.

6. Protection against GPS jamming:

Multi-channel receivers - the use of receivers that can work with several satellite navigation systems (GPS, GLONASS, Galileo, BeiDou) to reduce dependence on a single source.

Integration with inertial navigation systems (INS) - use of INS to maintain navigation accuracy in conditions of GPS signal jamming.

7. Jamming Detection and Localization.

Sensors and monitoring systems - implementation of sensors that can detect and analyze electronic jamming.

Localization of jamming sources - use of triangulation and spectrum analysis methods to determine the location of jamming sources and take measures to bypass or suppress them.

8. Swarm Coordination and Interaction.

Mutual coordination and relay communication - development of protocols for the exchange of information between drones in a swarm, which allows to maintain communication even when direct communication with the operator is disrupted.

Dynamic task assignment - the ability to redistribute tasks and roles in the swarm in real time to adapt to changing conditions and threats.

It is important to note that none of these methods is versatile, and the most effective approach will depend on the specific conditions of drone swarms and the threats that may potentially arise in the battle space.

To achieve maximum EW resistance, it is recommended to use a combination of different methods.

Conclusion

The course of russia's war against Ukraine, as well as the experience of other recent military conflicts, clearly shows the ever-increasing role of unmanned aerial vehicles in achieving results during operations (combat actions). At the same time, it is obvious that the forms and methods of their use require constant improvement and development. And the use of drone swarms in the realities of modern warfare is one of the priority directions for the development of the use of unmanned combat systems on the battlefield. At the same time, special attention should be paid to the perfection of the system for organizing communication and control of swarms of unmanned aerial vehicles (drones), which will ensure the highest level of efficiency of their use. The considered methods and technologies of communication and data exchange will allow to organize stable and uninterrupted control of swarms of unmanned aerial vehicles (drones).

Recommendations

For the sustainable use of unmanned aerial vehicles (drones) in the operations (combat actions) of the Defense Forces, it is necessary to solve the problems of optimizing the swarm control system according to the conditions of use, ensuring sustainable counteraction to the operation of enemy electronic warfare systems and functioning in all weather conditions. To achieve this goal, it is necessary to develop and implement algorithms for building drone swarm configurations in accordance with emerging tasks, to create a system for communicating drone swarm control with the introduction of modern technologies using artificial intelligence, which will, among other things, minimize the impact of enemy EW on unmanned aerial vehicles.

References

1. Gorbulin, V. P., & Mosov, S. P. (2024). Roji droniv – kul'minatsiya dronizatsiyi voien. *Visnik Natsional Noi Academii Nauk Ukrai Ni, (3),* 3–11. https://doi.org/10.15407/visn2024.03.003
2. Cabinet of Ministers of Ukraine. (2024, January 10). *"Army of Drones" year: Mass production of drones in Ukraine, strike UAV companies, and operator training—Key achievements of the project*. https://www.kmu.gov.ua/news/armii-droniv-rik-masove-vyrobnytstvo-droniv-v-ukraini-udarni-roty-bpla-navchannia-operatoriv-droniv-holovni-dosiahnennia-proektu
3. U.S. Government Accountability Office. (2023). *Uncrewed aircraft systems: FAA should improve its approach to integrating UAS into the national airspace system* (GAO-23-105189). https://www.gao.gov/assets/870/861345.pdf
4. *The Era of the Drone Swarm Is Coming, and We Need to Be Ready for It*. Modern War Institute (westpoint.edu). https://defensebridge.com/article/what-is-a-drone-swarm-an-overview-of-the-technology.html
5. Guo, J., Wang, L., & Wang, X. (2022). A Group Maintenance Method of Drone Swarm Considering System Mission Reliability. *Drones, 6,* 269.

https://doi.org/10.3390/drones6100269
6. Qiao, G., Zhuang, Y., Ye, T., & Qiao, Y. (2023). BCDAIoD: An Efficient Blockchain-Based Cross-Domain Authentication Scheme for Internet of Drones. *Drones*, *7*, 302. https://doi.org/10.3390/drones7050302
7. Mehmood, A., Iqbal, Z., Shah, A., Maple, C., & Lloret, J. (2023). An Intelligent Cluster-Based Communication System for Multi-Unmanned Aerial Vehicles for Searching and Rescuing. *Electronics*, *12*, 607. https://doi.org/10.3390/electronics12030607
8. Chen, J., Zhang, R., Zhao, H., Li, J., & He, J. (2023). Path Planning of Multiple Unmanned Aerial Vehicles Covering Multiple Regions Based on Minimum Consumption Ratio. *Aerospace*, *10*, 93. https://doi.org/10.3390/aerospace10020093
9. Wu, X., Zhang, M., Wang, X., Zheng, Y., & Yu, H. (2023). Hierarchical Task Assignment for Multi-UAV System in Large-Scale Group-to-Group Interception Scenarios. *Drones*, *7*, 560. https://doi.org/10.3390/drones7090560
10. Davoli, L., Pagliari, E., & Ferrari, G. (2021). Hybrid LoRa-IEEE 802.11s Opportunistic Mesh Networking for Flexible UAV Swarming. *Drones*, *5*, 26. https://doi.org/10.3390/drones5020026
11. Ganesan, T., Jayarajan, N., Shri, & Varun, B. G. (2024). *Dynamic Control, Architecture, and Communication Protocol for Swarm Unmanned Aerial Vehicles. Computing in Intelligent Transportation Systems.* EAI/Springer Innovations in Communication and Computing. https://doi.org/10.1007/978-3-031-38669-5_3
12. Krasavtsev, B. (2022). *Нові технології військових дронів для оборони України*. Ucluster. https://ucluster.org/blog/2022/06/vijsjkovi-drony-dlja-oborony-ukrainy/
13. Liang, O. (2021). *FPV Protocols Explained (CRSF, SBUS, DSHOT, ACCST, PPM, PWM*. Oscar Liang FPV Drone Tutorials and Reviews. https://oscarliang.com/rc-protocols/
14. Liang, O. (2021). *FPV Protocols Explained. Oscar Liang FPV Drone Tutorials and Reviews.* https://hinaray.com/understanding-the-communication-protocols-and-frequency-bands-used
15. Hopson, M. (2023). *How Does A Drone Communicate With Controller*. https://robots.net/tech/how-does-a-drone-communicate-with-controller/
16. Liang, O. (2021). *FPV Protocols Explained 1. Oscar Liang FPV Drone Tutorials and Reviews*. https://www.dronetrest.com/t/rc-radio-control-protocols-explained-pwm-ppm-pcm-sbus-ibus-dsmx-dsm2/1357

Проблематика організації зв'язку та управління роями безпілотних летальних апаратів (дронів)

Сергій Тараповський
начальник науково-дослідного відділу
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: tarapovskyi@gmail.com
ORCID: 0009-0004-4951-6056

Михайло Антонішин
науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: antonishin.mihail@gmail.com
ORCID: 0000-0002-2665-0066

Олексій Грамак
провідний науковий співробітник
Центральний науково-дослідний інститут Збройних Сил України
03049, проспект Повітряних Сил, 28 Б, Київ, Україна
e-mail: Hramakoleksij@gmail.com
ORCID: 0009-0008-5603-9779

Роман Войцеховський
ад'юнкт кафедри управління військами інституту державного військового управління
Національний університет оборони України
03049, проспект Повітряних Сил, 28, Київ, Україна
e-mail: voytsehovskiy31@gmail.com
ORCID: 0009-0000-6408-9620

Олег Тарасов
кандидат військових наук, доцент
доцент кафедри військової підготовки
Національний авіаційний університет
03058, проспект Любомира Гузара, 1, Київ, Україна
e-mail: tarasovo@ukr.net
ORCID: 0000-0002-6763-8653

Анотація. Стаття досліджує важливі аспекти організації зв'язку та управління роями безпілотних летальних апаратів (дронів). Автори розглядають проблеми, пов'язані з вирішенням завдань по забезпеченню безперебійного зв'язку в ході бойового застосування дронів, координації їх дій при виконанні завдань в режимі реального часу. В статті аналізуються різні підходи до вирішення цих проблем, а також надаються рекомендації щодо покращення ефективності управління роями дронів. Досвід використання безпілотних літальних апаратів під час повномасштабного вторгнення росії в Україну показав, що постійно виникає потреба у впровадженні нових підходів до застосування дронів, в тому числі використання роїв, які дозволять значно збільшити ефективність нанесення вогневого ураження противнику. І саме для роїв дронів критично важлива координація та злагодженість в процесі їх застосування. В залежності від способів застосування роїв дронів в системі управління розрізняють три основні підходи до керування ними: одиночне машинне управління, централізоване управління та розподілене управління. Для забезпечення безперервного управління роями дронів необхідно забезпечити стійкість та захищеність каналів управління роями дронів. Це досягається шляхом використання різних протоколів передачі даних, стандартів каналів зв'язку та здійснення шифрування даних.

Ключові слова: БпЛА, дрони, безпілотні системи, системи зв'язку, системи управління, безпілотні комплекси, стандарти управління, SUAV, LoRa, LoRaWAN, стандарт IEEE 802.11s, модуль SUCOM.