Research of UAV and sensor network integration features for routing optimization and energy consumption reduction

Nadiia Dovzhenko[1,†], Yevhen Ivanichenko[1,†], Pavlo Skladannyi[1,2,*,†] and Oleksii Zhyltsov[1,†]

[1] *Borys Grinchenko Kyiv Metropolitan University, 18/2 Bulvarno-Kudryavska str., 04053 Kyiv, Ukraine*

[2] *Institute of Mathematical Machines and Systems Problems of the National Academy of Sciences of Ukraine, 42 Ac. Glushkov ave., 03680 Kyiv, Ukraine*

Abstract

Modern unmanned aerial vehicles (UAVs) are increasingly integrating with sensor networks, significantly expanding the capabilities of real-time data collection, transmission, and processing. This integration is critically important for various sectors, including environmental monitoring, smart city infrastructure management, agriculture, and military operations. UAVs provide mobility and access to remote and hard-to-reach locations, enabling effective monitoring in areas where traditional networks are unavailable or ineffective. However, alongside these advantages, numerous technical challenges arise. These challenges include optimizing UAV flight routes to ensure maximum sensor network coverage, minimizing energy consumption, and addressing data security issues such as cyber threats. Another important aspect is flight duration, which depends on UAV battery capacity and energy-saving methods for sensor nodes, especially through the use of alternative energy sources, such as solar panels. The study presents a model of dynamic interaction between UAVs and a sensor network, examining the process of data collection, and transmission to a central server, and the impact of increasing the number of sensor nodes on the overall mission time. A stochastic model is proposed to account for environmental heterogeneities, such as data transmission delays caused by obstacles or changes in connection speed. An analysis is conducted to evaluate the impact of these factors on data collection efficiency and to optimize flight routes, with a focus on dynamic programming algorithms and heuristic methods.

Keywords

UAVs, drones, sensor networks, IoT, nodes, energy efficiency, routing, security, reliability, connectivity, data

1. Introduction

Unmanned aerial vehicles (UAVs) are increasingly being used in various fields of human activity. For example, in agriculture, GPS-guided UAVs are employed for spraying crops in the fields. The use of UAVs significantly saves resources (such as time and chemicals) and ensures accurate and precise treatment of agricultural lands compared to manned aviation [1].

In some European Union countries, drones are even used for customer deliveries. During military conflicts and wars, UAVs are utilized for delivering medications, humanitarian aid, and combat supplies to hard-to-reach areas. Certain drone models are also employed to inspect power lines, transformers, and pipelines [2].

Emergency services deploy drones for monitoring, forecasting, and controlling hazardous sites, contributing to both safety and environmental protection. In particular, UAVs can serve as platforms for meteorological measurement systems.

They have advantages over fixed-wing UAVs, whose high speed limits spatial and temporal resolution, making them less sensitive to turbulent processes [3].

Today, relatively affordable multicopters are available, capable of lifting payloads of 3–5 kg to altitudes of 2–4 km with flight durations of 30–40 minutes. Modern UAVs, equipped with onboard navigation and control systems, perform a wide range of functions. For example, UAVs can be programmed with fixed flight routes (using coordinates, altitude values, and specific waypoints) and can change their routes or return to the starting point upon command from the ground control station. Additionally, UAVs can fly over designated points, collect and transmit telemetry information about flight parameters and the operation of target equipment, and provide software control for this equipment [4].

CPITS-II 2024: Workshop on Cybersecurity Providing in Information and Telecommunication Systems II, October 26, 2024, Kyiv, Ukraine

* Corresponding author.

† These authors contributed equally.

nadezhdadovzhenko@gmail.com (N. Dovzhenko);
y.ivanichenko@kubg.edu.ua (Y. Ivanichenko);
p.skladannyi@kubg.edu.ua (P. Skladannyi);
o.zhyltsov@kubg.edu.ua (O. Zhyltsov)

0000-0003-4164-0066 (N. Dovzhenko);
0000-0002-6408-443X (Y. Ivanichenko);
0000-0002-7775-6039 (P. Skladannyi);
0000-0002-7253-5990 (O. Zhyltsov)

Moreover, modern UAVs are actively integrated into fields such as environmental monitoring, terrain mapping, and construction. Drones are also used in search and rescue operations and to assess agricultural land conditions. Advancements in artificial intelligence, sensor networks, and microchips have significantly improved the autonomy and accuracy of UAV flights, making them indispensable across many industries. This enables greater mobility and efficiency in operations while maintaining relatively low operational costs for UAVs [5].

2. Evolution, classification, and modern applications of unmanned aerial vehicles

Research in the field of unmanned aerial vehicles (UAVs) has a long and rich history. It began during World War I, in 1917–1918, with developments in the United States and the United Kingdom. One of the prototypes, the Kettering Bug, was an early cruise missile with a simple control system that allowed it to fly along a predetermined route. Another example, is the Aerial Target, an unmanned aircraft controlled via radio, which was developed for anti-aircraft artillery training. Although the project faced numerous technical limitations and was ultimately unsuccessful, it laid the foundation for further advancements in aviation.

During World War II, the German army deployed the first attack unmanned aerial vehicle (UAV)—the V-1 flying bomb. Later, researchers classified this aircraft, and its predecessors, as cruise missiles rather than conventional UAVs. However, it is important to note that their characteristics laid the groundwork for modern UAVs, particularly in terms of autonomy and the ability to accurately reach targets without a pilot.

From the 1950s to the 1970s, significant scientific research and development were conducted in the field of combat UAVs, particularly in versions capable of flying at high altitudes, remaining airborne for extended periods, and conducting surveillance. UAVs such as the Ryan Firebee, AQM-34 Ryan Model 147, and Teledyne Ryan AQM-91 Firefly were not only used for reconnaissance and training tasks but also represented advancements in remote control technologies that eventually became fully operational combat platforms.

Modern drones are used not only for military purposes, reconnaissance, and precision strikes but also for civilian tasks, such as search and rescue operations, infrastructure monitoring, agriculture, environmental monitoring, and cybersecurity. UAVs such as the RQ-1 Predator, MQ-9 Reaper, DJI Phantom, MQ-25 Stingray, Bayraktar TB2, Hermes 900, Wing Loong II, XQ-58A Valkyrie, and others have significantly expanded their capabilities thanks to the continuous development of artificial intelligence technologies, improvements in computing power, and the implementation of sensor systems [6].

Analyzing the existing varieties of unmanned aerial vehicles, they can generally be classified by their structural features. For example:

- Small UAVs are typically built based on classic aerodynamic designs, with variations such as "flying wings". These aircraft usually have high-mounted wings, often in a V-shape, with electric motors. They may also feature more complex fuselage designs—from gondolas to single-fuselage solutions. They are equipped with piston engines and typically take off from specially designed launch platforms. Their landing is accomplished either by parachute or via traditional aircraft methods. The advantage of such drones is their ability to perform much longer and more complex missions, remaining airborne for up to 5 hours.
- Medium UAVs have heavier landing gear and more complex takeoff and landing systems, which are more similar to traditional aviation principles. These drones can perform long-duration flights (approximately up to 20 hours) and can ascend to altitudes of up to 6 kilometers.
- Heavy UAVs are designed as "air giants" compared to other UAVs. They can reach altitudes of up to 20 kilometers and remain airborne for more than 24 hours. The construction of such UAVs involves the use of sufficiently complex and powerful engines and landing gear, making them effective for strategic missions and multifunctional tasks.

It is also appropriate to classify UAVs by weight, as this represents a separate classification for determining the capabilities of such devices. Small UAVs (weighing up to 5 kg) can perform short-term reconnaissance missions, such as target detection in hard-to-reach areas. Research indicates the potential for the weight of heavy UAVs to increase to 15 tons in the coming decades [7].

These options will be capable of performing strategic functions, combining reconnaissance, monitoring, and the management of a large amount of equipment for various tasks [8].

3. Technical aspects of integrating sensor networks and UAVs

The world of the Internet of Things (IoT) is broad and multifaceted, encompassing a wide range of industries, each with its own unique features and technological requirements. However, it is more appropriate to view IoT not as a single technological domain, but as a combination of different concepts, protocols, and technologies that vary depending on the application.

Sensor networks are a key component of IoT, providing monitoring of physical parameters of the environment. Due to limited resources and the need to operate in harsh conditions, these networks often face challenges such as node failures and malfunctions, leading to new issues, particularly in scaling the network to accommodate large numbers of connected devices, processing large volumes of data, and ensuring security.

Therefore, a logical step in the development of these technologies is the integration of UAVs with sensor networks, opening up new possibilities for efficient data collection, monitoring, and management in various areas of human activity, including the deployment of "smart" cities, environmental monitoring, critical infrastructure systems, cybersecurity, and even military applications.

One of the main advantages of using UAVs as mobile base stations is the improvement of communication between sensor nodes and drones, reducing signal loss, increasing the likelihood of direct line of sight, and, most importantly, decreasing the energy consumption of sensor resources. It is worth noting that sensor networks consist of hundreds or thousands of nodes that collect, process, and transmit data to central servers or cloud platforms using wireless communication protocols for further analysis.

Therefore, reducing energy consumption is especially important for nodes with low battery power, as it helps extend their operational life [9].

To ensure effective data collection and transmission between UAVs and sensor nodes, technologies such as LoRaWAN, Zigbee, and 5G are used.

For comparison, LoRaWAN and Zigbee provide stable communication in difficult conditions with low power consumption, extending the operational life of the sensors.

5G technology enables the transmission of large amounts of data in real time and ensures low latency, which is critical for tasks that require an immediate response.

Additionally, drones can be used to install sensor nodes in hard-to-reach or dangerous locations for humans, such as disaster zones, mountainous regions, seismically active areas, or sites of industrial accidents. In this case, the use of UAVs as mobile platforms for sensor networks allows for flexible positioning, data collection, and preliminary processing over large areas, providing continuous monitoring and rapid response to real-time changes [10].

Another key aspect of integrating sensor networks and UAVs is the optimization of drone flight paths to ensure maximum sensor network coverage while minimizing energy consumption. Key parameters that affect the efficiency of data collection include flight speed, distance to sensor nodes, transmitter power, flight altitude, and more.

The use of dynamic programming, heuristic algorithms, and machine learning methods enables the real-time optimization of drone routes, improving the performance of the data collection system and reducing the likelihood of errors or failures.

However, one of the biggest challenges remains the limited capacity of drone batteries, which determines their capabilities and flight duration. Due to several factors, lithium-ion batteries remain the most efficient; however, the issue of limited energy forces the search for new approaches and solutions. For example, new types of batteries, fuel cells, or hybrid power sources may be considered for drones. For sensor nodes, solar panels are used, reducing the frequency of recharging and ensuring continuous system operation. Energy-saving methods for sensor components, such as adaptive module shutdowns and optimization of data collection frequency, are also actively being researched [11].

Additionally, to ensure proper synchronization between sensor nodes and drones, especially in complex or dynamic environments, special routing algorithms, and dynamic data correction are used. Reliable synchronization is critically important to prevent data loss and ensure the stable operation of the entire system.

It is also worth noting the importance of cybersecurity, which is another key aspect of integrating UAVs and sensor networks. The use of modern encryption and authentication mechanisms helps prevent unauthorized access to data, which is especially important for military and industrial applications [12].

4. Model of dynamic interaction between UAVs and sensor networks

The integration of UAVs and sensor networks offers vast opportunities to improve efficiency and security in many sectors, but it also requires addressing several technical challenges to ensure the stable and reliable operation of such systems.

A model of the dynamics of data collection and interaction between UAVs and a sensor network is proposed, based on a specific scenario. In this scenario, the drone flies over several sensor nodes, collecting data from them and transmitting it to a central server. For modeling this process, a sensor network consisting of 50, 100, 200, or 500 nodes is considered. The time for data collection, data transmission, and command processing is also taken into account.

For example, the flight time to the sensor network nodes is determined by formula (1) and depends on the distance between the sensor nodes and their quantity.

$$t_f = \frac{d_s}{v_d}, \quad (1)$$

d_s is the distance between sensor nodes (e.g., 100 m), v_d is the speed of the drone (for example, 10 m/s). If the number of nodes increases but the area size remains unchanged, the distance between the nodes decreases proportionally.

This, in turn, will affect the flight time, reducing it, but increasing the number of nodes the drone interacts with and connects to [13].

The total interaction time between a sensor node and the drone is calculated as follows:

$$t_{total} = t_{data\ collection} + t_{data\ transfer} + t_{flight}, \quad (2)$$

where $t_{data\ collection}$ is time for data collection from a single node, $t_{data\ transfer}$ is time for data transfer from a single node, and t_{flight} is flight time.

The data transfer rate is determined as follows:

$$t_{data\ transfer} = \frac{R_{data}}{S_t}, \quad (3)$$

where R_{data} is data volume from one node (for example, 10 MB), and S_t is transfer speed (for example, 1 Mbit/s).

To formulate the mathematical model of the interaction between sensor nodes and UAVs (drones) in such a scenario, a system of equations can be used to describe the process of data collection, transmission, and processing from sensors, taking into account discrete time intervals.

The model will be based on stochastic process concepts to simulate random delays and heterogeneities [14].

The model for drone data collection and transmission can be described as a discrete process that defines the change in system state at the time t_n, when the drone moves between sensors and collects information:

$$X_{i,n+1} = X_{i,n} + \mu_{i,n} L_{i,n}(X_{i,n}\xi_{i,n}), \quad (4)$$

where $X_{i,n}$ is the volume of collected data at a given time t_n, $\mu_{i,n}$ is discretization step parameter, which regulates data state changes, $L_{i,n}(X_{i,n}\xi_{i,n})$ is a function that describes the process of data collection and transmission from sensor

node i under certain conditions, $\xi_{i,n}$ is models random delays or other changes in the system.

For a system with N sensor nodes, the total data collection time will be defined as:

$$T_G = N * t_{total}, \quad (5)$$

where N is the number of sensors, and t_{total} is the total interaction time with one sensor node.

The overall interaction time of the drone with the sensor network increases almost linearly with the number of sensor nodes, as shown in Fig. 1.

Each additional sensor node increases the total mission time due to the time required for flight, data collection, and data transmission to the gateway or server.

With a significant increase in the number of sensor nodes, optimization strategies should be considered, such as using multiple drones in parallel, dividing areas of responsibility, or using faster data transmission channels.

To optimize the route between sensor nodes, graph-based approaches or the traveling salesman problem can be used, where the drone must find the most efficient route that minimizes the distance between nodes.

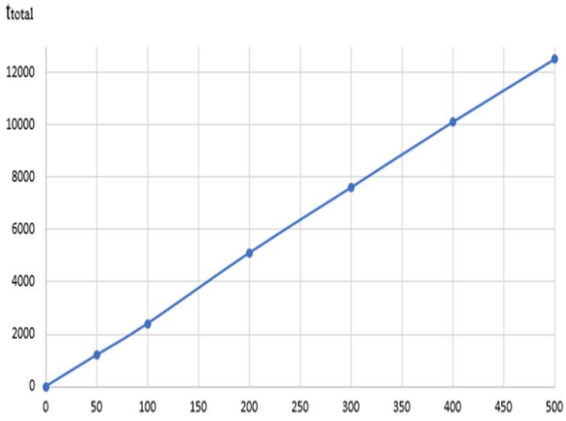

Figure 1: Dependence of total data collection time on the number of sensor nodes

From Fig. 1, it can be observed that as the number of sensors increases, the total time increases linearly, as the drone needs more time to fly over all the sensors, collect data, and transmit it to the server.

However, the presented calculations do not always reflect realistic scenarios. In real-world conditions, heterogeneities may arise, such as delays due to obstacles (e.g., trees, buildings, or other objects that may slow down the drone or cause additional energy expenditure), changes in data transmission speed (sometimes the speed may fluctuate due to interference, the distance between drones and the server, etc.), or variations in flight time due to differing distances between sensors (sensors may be distributed unevenly), and so on.

To account for such heterogeneities, random delays or variables can be added to the flight time, data collection, and information transmission time, for example:

$$t_f = \frac{d_s}{v_d} + \epsilon_f, \quad (6)$$

where ϵ_f is a random value of delay or change that creates heterogeneity.

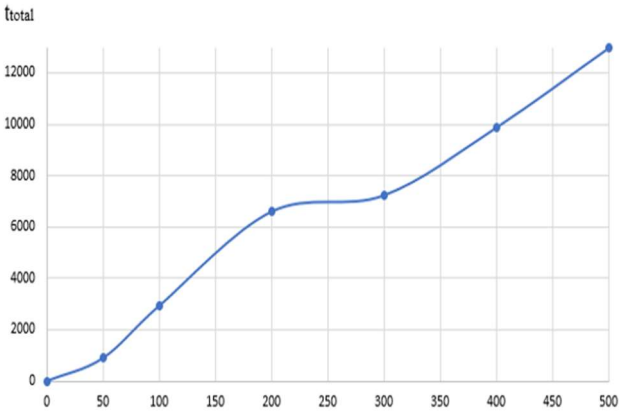

Figure 2: Dependence of total data collection time on the number of sensor nodes, considering heterogeneities in flight, data collection, and transmission times

Fig. 2 shows the heterogeneities accounted for in the time for flight, data collection, and transmission.

It can be argued that adding random variations in time simulates real conditions, where delays due to obstacles or changes in data transmission speed may occur [15].

5. Data Security Challenges in UAV-Integrated Sensor Networks

Since sensor networks and their components are often deployed in uncontrolled or insufficiently protected physical environments, especially in the case of integration with UAVs, it is crucial to pay particular attention to the impact of attacks and threats on both individual nodes/sensors and drones.

Due to the numerous advantages of UAVs interacting with sensor nodes, there is an increased risk of unauthorized access, data manipulation, or modification, as well as heightened vulnerability to the compromise of nodes and drones through physical access to network elements. In such cases, malicious software can be implanted, potentially compromising the integrity and confidentiality of the processed information. The aforementioned threats jeopardize not only individual network components but also the security of the entire system [16].

Today, there is a broad range of threats and types of attacks that can target sensor networks, occurring at various levels. One of the most common types of attacks is jamming, aimed at introducing additional noise and interference in the physical channel for wireless signal transmission, which can disrupt the correct interaction between nodes and UAVs. Other common threats include physical interference with network operations, sensor spoofing, or attacks on information leakage through direct access to network components. Such threats may lead to unpredictable consequences, including modification, delay, or loss of data sent to gateways, routers, or central servers, potentially causing misinformation or improper data processing.

For instance, at the link layer, a significant threat includes collision attacks, where identical frequency channels are used. Such attacks lead to resource depletion of nodes by forcing them to repeatedly retransmit damaged or lost packets to recipient nodes, ultimately negatively affecting network performance. When interacting with UAVs, these attacks can trigger excessive energy consumption by nodes, reducing the overall system uptime

and increasing the risk of node disconnections from the network.

At the network level, attackers can alter or spoof routing data, redirecting legitimate traffic to compromised nodes. An example is the Black Hole attack, in which a node intercepts data and does not forward it, creating a "black hole" in routing. Another example is the Selective Forwarding attack, where a malicious node selectively forwards only part of the packets, ignoring the rest. During interactions with UAVs, these attacks can cause serious disruptions in data delivery and negatively affect the timeliness of data receipt.

Additionally, sensor networks are vulnerable to eavesdropping and traffic analysis attacks, which allow attackers to access confidential information, modify it, or alter it for further attacks on the network. To mitigate risks associated with these threats, robust encryption and authentication methods must be employed to protect data transmitted between UAVs and sensor nodes.

Thus, ensuring the security of sensor network components, especially when used in conjunction with unmanned aerial vehicles (UAVs), is a highly challenging task due to the limited resources of each sensor. The constrained processing power, memory, and energy resources of sensor nodes create challenges for effective encryption key management, which is essential for data protection.

Modern strategies require the development of distribution and key-update mechanisms that can adapt to rapid network topology changes while maintaining a high level of security amidst constant UAV interaction. It is worth emphasizing that the dynamic nature of this topology also places additional demands on the speed of adaptation of security mechanisms.

As the number of sensor nodes increases, the load on data storage and transmission systems also rises, complicating security maintenance. The use of data compression technologies and selective data transmission algorithms can optimize network performance, reducing the volume of transmitted data and thereby shortening the period during which the network remains vulnerable to attacks.

However, resource limitations necessitate additional approaches to achieve comprehensive protection for sensor networks and UAVs.

To ensure protection at every level of the system, it is crucial to enable interaction between security mechanisms. For instance, effective energy resource management at the channel level can significantly reduce vulnerability to resource-depleting attacks, such as Denial of Service (DoS) attacks. For this purpose, it is beneficial to implement strengthened authentication and encryption protocols that provide additional protection against unauthorized access at the physical and network levels.

Modern encryption methods and advanced security algorithms at the network level allow for the prevention of routing data spoofing and protect the system from Black Hole and Selective Forwarding attacks. At the transport level, Flooding attacks and similar strategies targeting the depletion of node memory and computational resources represent another threat that must be taken into account.

Additionally, the threat of synchronization attacks should be considered, as such intrusions can disrupt data transmission and interfere with coordinated operations between sensors and UAVs.

In addition to the core information security goals (confidentiality, integrity, and availability), sensor networks also require secondary security objectives, such as data relevance, network self-organization capabilities, time synchronization, as well as node tracking and security incident localization. In the case of UAV integration, these aspects become critically important, as the constant movement of drones imposes additional requirements on the system's response time to potential threats.

Therefore, ensuring the security of wireless sensor networks when used with UAVs demands a comprehensive approach that includes multi-level protection against various types of attacks, adaptive resource management, and continuous improvement of security mechanisms to effectively counter emerging cyber threats [17].

6. Conclusions

The integration of unmanned aerial vehicles (UAVs) with sensor networks opens new opportunities for efficient data collection and transmission across various industries, particularly in remote and hard-to-reach locations. The results presented in this study indicate that such integration significantly enhances the quality of real-time monitoring and process management.

The proposed mathematical model describes a linear increase in total mission time as the number of sensor nodes grows, underscoring the need for optimizing UAV flight routes. Such optimization reduces interaction time with sensor nodes and improves data collection efficiency.

The study also examines the implementation of alternative power sources, such as solar panels for sensor nodes and hybrid batteries for UAVs. These solutions positively impact the system's continuous operation time and extend flight durations.

Additionally, special attention is given to data security, as the use of UAVs increases the risk of unauthorized access, manipulation, and attacks on the sensor network. Implementing multi-level protection mechanisms, adaptive resource management, and advanced encryption methods ensures data protection and system stability amid continuous UAV interactions.

References

[1] Z. Li, et al., An Adaptive and Automatic Power Supply Distribution System with Active Landmarks for Autonomous Mobile Robots, Sensors 24 (2024). doi: 10.3390/s24186152.

[2] J. Deng, et al., A Methodology to Monitor Urban Expansion and Green Space Change Using a Time Series of Multi-Sensor SPOT and Sentinel-2A Images, Remote Sens. 11 (2019) 1230. doi: 10.3390/rs11101230.

[3] N. Dovzhenko, et al., Comprehensive Analysis of Efficiency and Security Challenges in Sensor Network Routing, in: Cybersecurity Providing in Information and Telecommunication Systems II, vol. 3550 (2023) 275–280.

[4] N. Cheng, et al., AI for UAV-Assisted IoT Applications: A Comprehensive Review, IEEE Internet of Things Journal (2023). doi: 10.1109/JIOT.2023.3268316.

[5] K. P. Valavanis, G. J. Vachtsevanos, Handbook of Unmanned Aerial Vehicles, Springer Publishing Company, Incorporated (2014).

[6] J. M. Maddalon, et al., Perspectives on Unmanned Aircraft Classification for Civil Airworthiness Standards (No. NF1676L-16131) (2013).

[7] M. Asadpour, et al., Micro Aerial Vehicle networks: An Experimental Analysis of Challenges and Opportunities, IEEE Communications Magazine 52(7) (2014) 141–149. doi: 10.1109/MCOM.2014.6852096.

[8] N. Dovzhenko, et al., Method of Sensor Network Functioning under the Redistribution Condition of Requests between Nodes, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421 (2023) 278–283.

[9] M. Mozaffari, et al., A Tutorial on UAVs for Wireless Networks: Applications, Challenges, and Open Problems, IEEE Communications Surveys & Tutorials, 21(3) (2018) 2334–2360. doi: 10.1109/COMST.2019.2902862.

[10] E. Y. Song, G. J. FitzPatrick, K. B. Lee, Smart Sensors and Standard-based Interoperability in Smart Grids, IEEE Sensors J. 17(23) (2017). doi: 10.1109/JSEN.2017.2729893.

[11] A. Hassanien, et al., Signaling Strategies for Dual-function radar Communications: An Overview, IEEE Aerospace and Electronic Systems Magazine, 31(10) (2016) 36–45. doi: 10.1109/MAES.2016.150225.

[12] R. W. Beard, T. W. McLain, Small Unmanned Aircraft: Theory and Practice, Princeton, NJ, USA: Princeton Univ. Press (2012). doi: 10.1515/9781400840601.

[13] G. Liu, et al., Joint radar communication system design based on filter bank multicarrier modulation scheme, IET Radar, Sonar & Navigation, 17(1) (2022) doi: 10.1049/rsn2.12323.

[14] R. Beard, et al., Autonomous Vehicle Technologies for Small Fixed-Wing UAVs, J. Aerospace Comput. Inf. Commun. 2(1) (2005) 92–108. doi: 10.2514/1.8371.

[15] O. Barabash, et al., Development of a hybrid network traffic load management mechanism using smart components, in: IEEE 7th International Conference on Methods and Systems of Navigation and Motion Control (MSNMC) (2023) 38–41.

[16] Z. Hu, et al., Analytical Assessment of Security Level of Distributed and Scalable Computer Systems. International Journal of Intelligent Systems and Applications, vol. 8, no. 12 (2016) 57–64.

[17] P. Openko, et al., Zabezpechennia nadiinosti ta bezpeky u suchasnykh bezprovodovykh sensornykh merezhakh na osnovi vprovadzhennia metryky RSSI. Povitriana mits Ukrainy, 1(6) (2024) 131–136. doi: 10.33099/2786-7714-2024-1-6-131-136