UDC: 004.9:004.056 https://doi.org/10.15407/jai2024.04.151

I. Rozlomii[1], A. Yarmilko[2], S. Naumenko[3]
[1]Cherkasy State Technological University, Ukraine
460, Shevchenka blv., Cherkasy, 18006
[2,3]Bohdan Khmelnytsky National University of Cherkasy, Ukraine
81, Shevchenka blv., Cherkasy, 18031
[1]inna-roz@ukr.net
[2]a-ja@ukr.net
[3]naumenko.serhii1122@vu.cdu.edu.ua
[1]https://orcid.org/0000-0001-5065-9004
[2]https://orcid.org/0000-0003-2062-2694
[3]https://orcid.org/0000-0002-6337-1605

THE INTELLIGENT APPROACHES TO ORGANIZING SECURE INFORMATION EXCHANGE IN DYNAMIC SWARMS OF UNMANNED PLATFORMS

Abstract. The article focuses on addressing the issue of data protection in the context of dynamic network topology and limited resources. In modern systems of autonomous unmanned platforms, the key task is to ensure reliable, secure, and energy-efficient information exchange between agents in conditions of constant changes in the swarm structure. The approaches proposed in the article include the use of lightweight cryptographic algorithms SIMON and SPECK, which provide minimal data transmission delays, low power consumption, and high resistance to attacks at the interception and modification level. The Q-learning algorithm, which allows agents to quickly adapt to changes in network topology, is discussed. Simulations conducted using the NS-3 platform demonstrated the advantage of intelligent approaches based on self-learning and cooperative decision-making methods in ensuring high system performance with minimal energy consumption and rapid adaptation to environmental changes. Security assessments confirmed the system's resilience to routing and data interception attacks, making these methods promising for further use in autonomous unmanned platforms.

Keywords: intelligent algorithms, unmanned platforms, secure data exchange, lightweight encryption protocols, self-learning, dynamic swarms, cooperation algorithms.

Introduction

An integral part of ensuring reliable information exchange between unmanned platforms is the organization of interaction within a swarm, where each agent can adapt to changing conditions and system structures in real time [1]. Such adaptability requires the use of intelligent algorithms and the development of new approaches to information security, allowing for effective solutions to resistance against attacks and ensuring high performance during task execution. Modern communication methods must not only guarantee the reliability of data exchange but also be resilient to failures and cyber threats. Special attention is drawn to the issue of data protection in dynamic swarms, whose structure is constantly changing [2]. To support the execution of cooperative tasks by such structures, new approaches to processing, transmitting, and securing information need to be developed, enabling adaptation to changes in the group structure.

Secure data exchange in autonomous systems is a critical aspect for many applications of unmanned platforms, particularly in defense, scientific research, and industry [3]. The implementation of intelligent solutions that integrate advanced artificial intelligence methods, machine learning algorithms, and adaptive communication models can significantly enhance the overall security and reliability of such systems.

Statement of the problem

The task of ensuring reliable and secure communication in dynamic swarms of unmanned platforms is to provide continuous and secure information exchange among individual autonomous agents within the swarm in conditions of dynamic structural changes. Possible solutions must take into account the resource limitations of the target platforms while ensuring information security and preventing overloads of onboard systems in terms of computational and energy capabilities. This requires the development of new approaches to encryption, authentication, and routing that correspond to the specifics of the dynamic environment while being resource-efficient. Agents must be able to adapt to real-time changes, minimizing data exchange delays and ensuring resilience against potential attacks.

To address this task, it is necessary to integrate intelligent algorithms, particularly self-learning methods, that allow autonomous agents to make independent decisions regarding route selection and encryption mechanisms depending on current conditions. Additionally, effective methods for dynamic key distribution should be developed to maintain a high level of security even during changes in the swarm's structure.

Analysis of recent research and publications

Within the study of secure information exchange in unmanned platforms, there is a significant body of scientific work dedicated to organizing interactions between autonomous agents and ensuring data security in dynamic networks. Research in this field covers various aspects, ranging from routing algorithms to encryption protocols for protecting data under resource constraints.

Particularly noteworthy are studies that explore the use of artificial intelligence to optimize data exchange in autonomous systems [4]. Specifically, the application of machine learning methods for adaptive routing and real-time decision-making is proposed [5]. These approaches significantly enhance the efficiency of unmanned platforms in changing conditions, ensuring network resilience to external threats. Research on the implementation of self-learning algorithms in the context of secure message exchange in dynamic swarms shows promising results, although questions about their effectiveness in complex scenarios remain open [6].

Research [7] focus on the development of lightweight cryptographic protocols for data protection in unmanned platforms. In this area, a number of studies have been conducted on the implementation of cryptographic algorithms with minimal energy consumption, which is critical for resource-constrained platforms. At the same time, the challenges related to balancing a high level of security and minimizing data transmission delays require further research. In [8] was emphasizes that existing solutions do not always provide an optimal balance between security and performance, especially under conditions of rapidly changing network topology.

Despite significant progress in the research of dynamic unmanned systems, some important issues remain unresolved. One such issue is ensuring communication resilience against a wide range of attacks, including routing-level attacks and packet manipulation. Additionally, the development of more efficient protection methods in the context of constant changes in system topology and reducing response time to changing conditions is of interest. Furthermore, there is still a need for further research on the impact of the latest security protocols on the overall system performance.

The aim of the research

The aim of the research is to develop intelligent approaches to organizing secure information exchange in dynamic swarms of unmanned platforms that ensure reliable and efficient data exchange under conditions of changing system topology and limited resources. Special attention is given to the implementation of artificial intelligence methods for automating decision-making, enhancing resilience to security threats, and ensuring stable platform operation in real-time.

An overview of the main material

The organization of effective and secure information exchange in swarms of unmanned platforms is a crucial component for the successful operation of these systems. The interaction between autonomous agents within the swarm must be coordinated and reliable, as each agent performs its tasks based on the information received from other participants.

Modern communication models used for information exchange in swarms of unmanned platforms are based on the principles of decentralization and autonomy. Each agent in the system operates independently, making decisions based on information received from other platforms.

The decentralized structure provides a high level of flexibility and adaptability, speeding up the swarm's response to changes in the environment or new tasks.

Swarm behavior of unmanned systems relies on the application of specialized coordination algorithms that enable the platforms to interact as a unified system. The primary methods for organizing such interaction include the use of collective intelligence and self-learning algorithms. Through these approaches, each agent not only fulfills its tasks but also contributes to achieving the overall goal of the swarm.

Figure 1 illustrates the swarm coordination algorithm, demonstrating the task distribution process among the platforms, as well as the coordination of actions for the seamless operation of the entire system. Self-learning algorithms help agents adapt their actions according to changing conditions, enhancing the effectiveness and accuracy of task execution in real-time. Coordination ensures the smooth functioning of the entire swarm, allowing each platform to perform its part of the task while minimizing the risk of duplicated actions or conflicts in resource distribution. This approach maintains a balance between the autonomy of each agent and the need for collective interaction, significantly enhancing the overall performance and reliability of the system.

Security challenges in information exchange are among the most critical issues faced by developers of swarm unmanned systems. Ensuring secure and reliable communication between autonomous agents becomes increasingly complex in the context of dynamic changes in network topology, the failure of individual platforms, and their limited resources. Specifically, the risks of data loss or delays in transmission may be caused by:

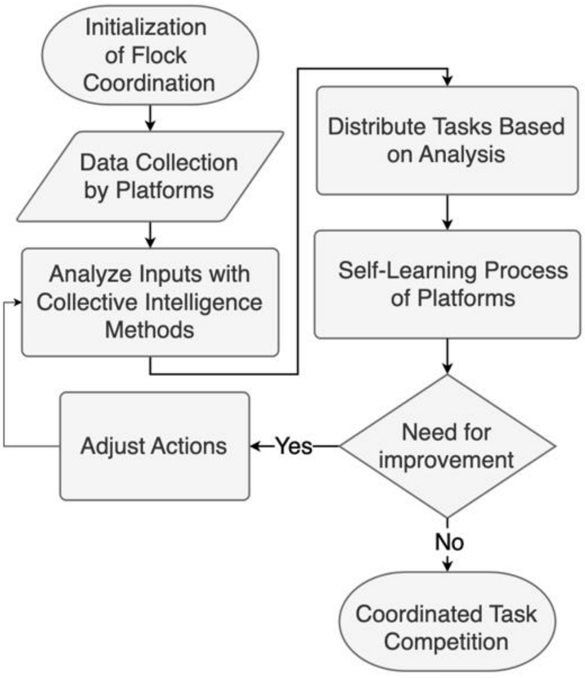
Initialization of Flock Coordination
Data Collection by Platforms
Analyze Inputs with Collective Intelligence Methods
Distribute Tasks Based on Analysis
Self-Learning Process of Platforms
Need for improvement
Yes
Adjust Actions
No
Coordinated Task Competition

Fig. 2. Flowchart of the swarm coordination algorithm

– spatial movements of unmanned platforms and loss of connectivity;

– the inability of other platforms to quickly compensate for the loss of some and continue effective interaction;

– the impossibility of applying complex cryptographic methods to protect information in the absence of sufficient onboard computing power;

– interception of information in unprotected data transmission channels and its modification;

– routing-level attacks and related disruptions in data streams, denial of service for individual platforms, and the emergence of vulnerabilities in the system to further attacks.

These challenges complicate the maintenance of a continuous flow of information and require the implementation of comprehensive solutions capable of not only protecting data from potential threats but also ensuring the flexibility and adaptability of the system to dynamic changes in the network of unmanned platforms. Alongside the development and integration of lightweight cryptographic algorithms and effective authentication mechanisms into unmanned systems, AI can play a key role in addressing routing, coordination, and data security issues due to its ability to analyze large volumes of data and find the most optimal solutions in real time.

Various algorithms are used in dynamic systems to optimize routes. These include algorithms based on classical shortest path search methods, bio-inspired algorithms, and machine learning-based algorithms. Each has its advantages and disadvantages, depending on the conditions and requirements of the specific system (Table 1). These algorithms are used for various types of tasks in unmanned platforms and help find a balance between performance, speed, and reliability [9]. For example, A* works effectively when finding the shortest path in a complex environment, while Q-learning allows the system to adapt to changes and autonomously find optimal routes based on past experiences [10, 11]. The use of artificial intelligence algorithms in routing not only improves data exchange efficiency but also ensures system flexibility in the face of constant environmental changes.

Table 1. Key properties of algorithms for route optimization in dynamic systems

Algorithm	Algorithm Type	Advantages	Disadvantages
A* (A-star)	Heuristic Algorithm	Fast optimal route search, effective in complex graphs	Can be slow for large networks
Dijkstra	Shortest Path Algorithm	Finds the shortest route from any point	Requires a lot of resources for large networks
Ant Colony Optimization (ACO)	Bio-inspired Algorithm	Effective in dynamic conditions, quickly adapts to changes	Requires more time to gather data for effective routing
Genetic Algorithm	Evolutionary Algorithm	Suitable for finding global solutions, works in unpredictable environments	High computational complexity, requires many iterations
Q-Learning	Reinforcement Learning	Self-learning based on rewards, adapts well to changes	Requires significant training time in large networks
Particle Swarm Optimization (PSO)	Bio-inspired Algorithm	Collective decision-making, effective for distributed systems	May not find a globally optimal solution
Distance-based Protocol	Routing Protocol	Simple implementation, minimal resource requirements	Can lead to suboptimal solutions in the case of dynamic changes

Self-learning algorithms and principles of cooperative decision-making are key components in building dynamic autonomous systems, particularly in unmanned platforms operating in swarms. Self-learning enables autonomous agents to improve their actions based on feedback from the environment during operation. One of the most popular approaches to self-learning is the Q-learning algorithm, which belongs to reinforcement learning methods. In the context of swarm unmanned systems, this algorithm allows each agent to select optimal actions to achieve its goals while adapting to changes in the environment and interacting with other agents [11].

Q-learning is based on the evaluation of the reward function $Q(s, a)$, which calculates the expected reward for performing action a in state s. The model is updated according to the following dependency:

$$Q(s_t, a_t) \leftarrow Q(s_t, a_t) + \\ +\alpha[r_t + \Upsilon \max_{a'} Q(s_{t+1}, a') - Q(s_t, a_t)], \quad (1)$$

where α – is the learning rate, r_t – is the reward received for action a_t, Υ – is the discount factor for future rewards, and $\max_{a'} Q(s_{t+1}, a')$ – is the maximum value Q for the next state. This formula allows the agent to evaluate how advantageous it is to perform a certain action in each state, enabling decision-making based on accumulated experience.

In systems with unmanned platforms, a crucial aspect is collective work, where each agent must make decisions considering the actions of other agents to achieve a common goal. Principles of cooperative decision-making allow each agent to adapt its behavior by coordinating with other members of the swarm, ensuring coherence in task execution.

The model of cooperative decision-making can be described using game theory, where each agent is considered a player, and the outcomes depend on the decisions of other players. The simplest model is a non-zero-sum game, where each player's gain depends on cooperation with others.

For each agent i, the utility function U_i is defined by the expression:

$$U_i(a_1, a_2, \dots, a_n) = R_i - C_i, \qquad (2)$$

where $a_{1,} a_2, \dots, a_n$ – are the agents actions, R_i – is the reward for agent i, C_i – is the cost of performing the action. The task of each agent is to maximize its utility function considering the actions of other agents. To achieve a cooperative solution, each agent can employ coordination strategies by exchanging information with other agents and aligning their actions.

The combination of self-learning and cooperative decision-making allows for the creation of a more adaptive and effective swarm management system for unmanned platforms. The model of cooperative Q-learning enables each agent not only to learn based on its actions but also to take into account information received from other agents. This enhances the efficiency of the system, reduces the risk of conflicts, and optimizes resource utilization in dynamic conditions.

Thus, the integration of self-learning and cooperative decision-making forms the foundation for developing intelligent dynamic systems capable of operating effectively in changing environments and ensuring reliable information exchange among agents.

Secure information exchange in swarms of unmanned platforms is based on the application of lightweight encryption and authentication protocols that ensure the confidentiality and integrity of transmitted data. Such protocols must be energy-efficient and computationally simple, given the limited resources of unmanned systems.

One widely used protocol is the Advanced Encryption Standard (AES), which provides high-speed encryption with minimal resource overhead. However, in the case of unmanned platforms, it is more appropriate to use lightweight variants such as SIMON, SPECK, or PRESENT, which are specifically designed for resource-constrained systems. Additionally, the use of authentication mechanisms, such as Hash-based Message Authentication Code (HMAC), is important for verifying data integrity [13].

Ensuring information protection under limited resources requires the use of distributed methods that allow for efficient utilization of the available computational power and energy resources of each agent in the swarm. One such approach is distributed encryption, where the encryption and decryption process is shared among multiple agents. This helps to reduce the load on each individual node and enhance the overall security of the network. Key management methods are also employed to ensure the dynamic distribution of encryption keys among agents. This ensures that only authorized platforms can access confidential information, even in the event of changes in the swarm's structure [14].

Dynamic key distribution means that each agent must obtain a unique or shared key for encrypting/decrypting data, with keys being able to change in response to changes in the network, such as the addition or removal of agents. One way to represent the dynamic key distribution process is to use a key generation function based on a shared secret:

$$K_i = f(K_s, ID_i), \qquad (3)$$

where K_i – is the agent's key i, K_s – is the shared secret key for the entire group, ID_i – is the unique identifier of the agent i, f – is a cryptographic function for key generation. The function f can be a hash function or another encryption algorithm that ensures the keys are unique for each agent and will change in the event of changes in the network topology. This approach ensures that only authorized agents have access to confidential data, even in the event of changes in the swarm's structure.

One of the methods used for dynamic key distribution in resource-constrained networks with dynamic topology changes is the Localized Encryption and Authentication Protocol (LEAP). It employs several types of keys: local, group, and pairwise keys. Each agent has multiple keys that are used for encryption in different contexts: for local encryption between two neighboring agents, for group encryption among all members of the swarm, and for individual pairwise keys for communication with a controller or base station. Keys are updated when an agent leaves or joins the network.

Since changes in the swarm structure are common in the dynamic operational conditions of unmanned platforms, it is crucial to ensure continuous and secure data exchange among agents despite changes in their number or locations. To achieve this, adaptive encryption is advisable, allowing the system to automatically adjust the level of protection based on the current network structure. This minimizes the risks of information leakage during moments when agents change their positions in the swarm or temporarily exit the network. Mobile agents are also employed to handle the redistribution of encryption and authentication keys during changes in the swarm structure. This helps maintain network integrity and ensures protection even in the event of unexpected changes in the system's topology.

With the advancement of unmanned platforms, autonomous systems increasingly rely on the ability to temporarily cluster into dynamic groups for cooperative tasks. The organization of dynamic clusters enhances the efficiency of autonomous agents and ensures quick responses to various real-time situations. Each agent in a cluster performs its part of the task, utilizing information from other cluster members to coordinate its actions. This organization allows for the distribution of complex tasks among several unmanned platforms, improving execution efficiency and minimizing the time required for their realization.

Among the most effective methods for organizing clusters are those based on collective intelligence, where agents autonomously determine their roles in task execution based on available information about the current environment. This enables dynamic adjustments to the cluster structure depending on task execution conditions, such as the presence of obstacles or changes in objectives.

To evaluate the effectiveness of various intelligent approaches in ensuring the security and performance of the system, simulations of data exchange in dynamic swarms of unmanned platforms were conducted. Platforms such as NS-3 and MATLAB were used, enabling accurate reproduction of network topology changes, agent behavior, and the constraints of their resources. NS-3 is widely used for modeling wireless networks and studying encryption and routing protocols. The mobility models of unmanned platforms were configured using the UAVMobilityModel, which allows for the simulation of agent movement in space. MATLAB software was used to analyze quantitative metrics, including transmission delay, throughput, energy consumption, and resilience to attacks.

The modeling showed varying effectiveness of applying intelligent approaches depending on the encryption protocols and routing algorithms:

– the lowest latency was achieved using the SIMON and SPECK algorithms, with respective latencies of 85 ms and 90 ms, compared to 120 ms for AES;

– the most energy-efficient were SIMON and SPECK, with an average consumption of 1.8 J per data transmission operation, while AES consumed about 2.5 J;

– the use of lightweight ciphers also resulted in a reduction of lost packets to 3% for SIMON and SPECK, compared to 5% for AES;

– the HMAC protocol used for

authentication demonstrated a high level of resistance to attacks, reducing the probability of successful routing-level attacks to 1%.

Thus, lightweight encryption protocols like SIMON and SPECK exhibit high resistance to data interception and modification. Even in cases where some agents were lost, the modeled system demonstrated stable performance. Thanks to the use of self-learning algorithms, particularly Q-learning, agents were able to quickly adapt to dynamic changes in the network, minimizing data transmission delays. This ensured continuous and secure information exchange even under challenging conditions.

The system's performance also remained high. The use of Q-learning and cooperative decision-making methods allowed for optimal results with minimal energy expenditure and high data exchange speed. The lowest latency and energy consumption were observed when using the SIMON and SPECK protocols, making them the most suitable for deployment in resource-constrained systems.

The modeling confirmed that self-learning and cooperative-based intelligent approaches are the most effective for ensuring productive and secure data exchange in dynamic swarms of unmanned platforms.

Conclusions

The conducted research demonstrated the high effectiveness of intelligent approaches for organizing secure information exchange in dynamic swarms of unmanned platforms. The use of lightweight cryptographic algorithms, such as SIMON and SPECK, ensures minimal delays in data transmission and low energy consumption, which is a critical factor for resource-constrained systems. The integration of self-learning algorithms, particularly Q-learning, has increased the system's flexibility and ensured stable performance even under constant changes in network topology.

The proposed approaches hold promise for further application in both scientific research and practical implementations. Utilizing lightweight ciphers and adaptive routing algorithms will enable effective security measures in resource-limited and variable environments. Special attention should be given to the development of autonomous vehicle systems, where dynamic operational conditions require rapid adaptation and reliable data exchange. Additionally, these approaches could be beneficial in fields such as military unmanned systems, energy-efficient communication networks, and logistics and search-and-rescue operations.

Future research should focus on further optimizing key distribution processes among agents in dynamic environments, particularly by developing new mechanisms to ensure resilience against complex types of attacks, such as routing-level attacks. It is also necessary to explore the potential for integrating cutting-edge machine learning algorithms to improve data processing speed and reduce energy consumption without compromising security levels. The continued development of distributed encryption and key management systems will enhance the overall resilience of the system against environmental changes and malicious attacks.

References

1. Raja, G., Anbalagan, S., Ganapathisub-ramaniyan, A., Selvakumar, M. S., Bashir, A. K., & Mumtaz, S. (2021). Efficient and secured swarm pattern multi-UAV communication. IEEE Transactions on vehicular technology, 70(7), 7050-7058.
2. Kallenborn, Z. (2022). InfoSwarms: Drone swarms and information warfare. The US Army War College Quarterly: Parameters, 52(2), 87-102.
3. Lehto, M., & Hutchinson, B. (2020, March). Mini-drones swarms and their potential in conflict situations. In 15th international conference on cyber warfare and security (Vol. 12, pp. 326-334).
4. Chen, J., Sun, J., & Wang, G. (2022). From unmanned systems to autonomous intelligent systems. Engineering, 12, 16-19.
5. Mao, B., Tang, F., Fadlullah, Z. M., & Kato, N. (2019). An intelligent route computation approach based on real-time deep learning strategy for software defined communication systems. IEEE Transactions on Emerging Topics in Computing, 9(3), 1554-1565.
6. Yarmilko A. V., Nikitiuk V. S. (2021) Modeliuvannia hrupovoi povedinky avtonomnyh ahentav za stsenariiem konsolidatsii. Visnyk KrNU imeni Mykhaila Ostrohradskoho. 6(131). 66–72. DOI: 10.30929/1995-0519.2021.6.66-72. [in Ukrainian]
7. Deebak, B. D., & Al-Turjman, F. (2020). A smart lightweight privacy preservation scheme for IoT-based UAV communication systems. Computer Communications, 162, 102-117.
8. Yarmilko, A., Rozlomii, I., Naumenko, S. (2024). Dependability of Embedded Systems in the Industrial Internet of Things: Information Security and

Reliability of the Communication Cluster. In: Faure, E., et al.Information Technology for Education, Science, and Technics. ITEST 2024. Lecture Notes on Data Engineering and Communications Technologies, vol 222, pp. 235–249. Springer, Cham. https://doi.org/10.1007/978-3-031-71804-5_16

9. Herlambang, T., Rahmalia, D., & Yulianto, T. (2019, April). Particle swarm optimization (pso) and ant colony optimization (aco) for optimizing pid parameters on autonomous underwater vehicle (auv) control system. In Journal of Physics: Conference Series (Vol. 1211, No. 1, p. 012039). IOP Publishing.

10. Pasandi, L., Hooshmand, M., & Rahbar, M. (2021). Modified A* Algorithm integrated with ant colony optimization for multi-objective route-finding; case study: Yazd. Applied Soft Computing, 113, 107877.

11. Liu, J., Wang, Q., He, C., Jaffrès-Runser, K., Xu, Y., Li, Z., & Xu, Y. (2020). QMR: Q-learning based multi-objective optimization routing protocol for flying ad hoc networks. Computer Communications, 150, 304-316.

12. Rozlomii, I., Yarmilko, A., & Naumenko, S. (2024, April). Data security of IoT devices with limited resources: challenges and potential solutions. In door (pp. 85-96).

13. Mitsenko, S., Naumenko, S., Rozlomii, I. & Yarmilko, A. (2023). Information Protection and Recovery Hamming Codes Based'Hash Technique. In Proceedings of the 11-th International Conference" Information Control Systems & Technologies" (Vol. 3513, pp. 64-67).

14. Bansal, G., & Sikdar, B. (2021). S-MAPS: Scalable mutual authentication protocol for dynamic UAV swarms. IEEE Transactions on Vehicular Technology, 70(11), 12088-12100.

15. Lamba, M. A., Tamrakar, M. G., & Gaur, M. H. (2022). Simulation of a UAV-based wireless sensor network on NS-3 to analyze IEEE 802.11 performance. Mathematical Statistician and Engineering Applications, 71(4), 6722-6737.

The article has been sent to the editors 18.10.24.
After processing 26.10.24.
Submitted for printing 30.12.24.