UDC 004.62; 004.75 **doi: 10.26906/SUNZ.2023.2.031**

Naghiyeva Parvin Abdulla

Baku State University, Baku, Azerbaijan

THEORETICAL ANALYSIS OF THE LEVEL OF COMMUNICATION SECURITY OF UAVS OPERATING AS PART OF A GROUP PERFORMING A COMBAT MISSION

Abstract. The research relevance lies in the issue of information impact on the AI of the drone and its vulnerability in order to perform sabotage actions by the enemy in local military conflicts. The article provides a theoretical analysis of the security of the information transmitted to a group of drones in order to establish the susceptibility of drones to false data and further organizational actions that can prevent the sabotage actions committed by the enemy and his allies, as well as analyzes situations when an aircraft is misinformed, which in turn entails the failure of the task by the entire group of drones. The subject and the purpose of the research is to establish the existence of the fact of misinformation by the enemy of the UAV, controlled remotely and performing a combat mission as part of a group without the direct participation of the operator. In the process of modeling the situation, theoretical analyzes of the behavior of the UAV were carried out, since the artificial intelligence in one aircraft is only able to influence its behavior and is not able, under false information impact, to establish the fact of false interference by the enemy in another drone in-group in the course of combat operations and warn other elements of the system in its group. Research methods are theoretical analyses of the communicative interaction of a swarm of drones based on the study of the research of algorithms of operator control. Obtained results and conclusion: encrypted false information transmitted with the aim of disorienting the UAV cannot be detected in advance by the classical approach to preventing cyber-attacks. In this regard, the problem of information security of drone AI remains relevant and requires further comprehensive theoretical and practical research with the involvement of IT specialists, linguists, engineers, and military experts.

Keywords: unmanned aerial vehicle, group of unmanned aerial vehicles, artificial intelligence, information security, data transmission.

Introduction

Currently, armed UAVs play an essential role in military operations during any local military conflicts. The situation in the Second Karabakh war in 2020 clearly showed and gave the idea to AI developers, engineers, and UAV designers that today remotely controlled aircraft can perform the combat missions which a few decades ago required numerous ground combat equipment, a professional army, and people`s lives [1-6].

Unmanned aviation of states with a small professional army can not only participate in local confrontations with minimal damage to military personnel but also act as allies of other states in the international arena [7].

Ground operations are gradually moving to combat missions conducted in the air, namely, drones can solve the issue of the speed of the military conflict, reduce losses on both sides, and provide comprehensive surveillance and reconnaissance of military areas.

For the purposes of this study, the author sets the task to determine whether the enemy has a remotely controlled UAV performing combat tasks in a group without direct participants, the fact of sabotage against a drone that can provoke disruption in the work of the entire drone group, and, consequently, losses and failure in completion of the task.

The subject of the study is false information transmitted to a drone operating in a group that performs combat missions with no human factor.

The relevance of the study lies in the issue of information influence on the AI of drones and their vulnerability. The research method consists in a theoretical analysis of the communicative relationship of a drone group based on operator control algorithms. To determine if there is a vulnerability in the system of a remotely controlled drone that performs combat missions in a group the analysis of the transmitted data has been carried out.

The results of the research [8] show that the issue of informational support of the drone performing the task in the group, as well as the entire group of drones, is the most important factor influencing the performance of the task, and requires developers to strengthen security systems against various enemy programs. Encrypted false data transmitted for the purpose of disinformation of UAVs cannot reveal the classic approach to preventing cyber-attacks in advance. The problem of drone information security currently remains relevant and will require further comprehensive theoretical and practical research with the participation of IT experts, engineers, linguists, and military specialists.

Practical value. The theoretical assessment of drone behavior in the situation, when it receives false information and its further interaction with other drones in the group, can be used for deeper practical research and the development of new methods for the security of transmitted information in order to eliminate vulnerabilities in the AI control system in the future local wars.

The second Karabakh war in 2020 clearly showed the civilized world that the speed of high-tempo combat engagements increased due to AI-enabled ISR and rapid command and control. Like any robotic equipment, UAVs have a number of vulnerabilities, and the efficiency of the equipment is to obtain reliable data and true information in order to complete the tasks assigned to the AI. At each stage of software development, there are a number of information security issues, so the main aim of this article is to analyze simulated situations when a drone receives false information and starts to perform a task based on that false information.

To reduce the risk of obtaining false data channels are analyzed for the presence of the threat of sabotage in the papers [9]. the results of the research confirm that in order to reduce the risk of obtaining false data, it is necessary to use a cryptographic encryption method.

The study [10] analyzed standard data management between drones, as well as between a drone and a human operator. According to the results of the research, AI is able to control remotely in real-time, but the standard way of transmitting information without any proper data security cannot be applied to military purposes, that is for reconnaissance, etc. due to the rather vulnerable transmission system.

Research [11] considers the issue of a group of drones, as well as an unmanned surveillance and reconnaissance aerial vehicle controlled from a ground control station (GCS). The analysis showed the vulnerabilities of communication channels, as well as the swarm of drones, that indicate cyberattacks of opponents aimed at diversification. The information received is intended for centralized control of the swarm, so it is not relevant for decentralized or single UAV control.

The author also notes dissertation research [12], which analyzes the drone network on its information vulnerability and its susceptibility to various cyber-attacks. Namely, the paper discusses the methods of organizing unmanned networks in civil and military aviation, but there is no analysis of the decentralized control of UAVs in combat situations.

Analyzing the above researches on ensuring information security, as well as on the level of security, the author assumes that identifying a vulnerability in the field of information security of combat UAVs is a key task at the development stage, as well as an integrated approach to the development of AI systems used for military purposes.

Therefore, the following tasks are formulated:

1. Analysis of existing approaches and research studies in the field of developing drone information security within the group;

2. Develop an algorithm for modeling the interaction of UAV groups, taking into account the data and conclusions of existing experiments;

To accomplish the stated tasks, it is necessary to apply new approaches to data transmission, and a comprehensive analysis of the existing interaction system, since the proposed and existing concept is not able to protect drones from cyber-attacks, and the main task of the drone is to perform the task transmitted via the communication channel.

Centralized control of a drone swarm. The main difference between centralized and decentralized control is the presence of a system that comprehensively controls the performance of drones while conducting combat missions. This element controls all the elements in the swarm system. The main advantage of this information and communication interaction of the drone is the synchronization of tasks using AI algorithms, but this control method has a number of vulnerabilities.

Let us consider the vulnerabilities:

1. If a swarm consists of a significant number of UAVs, the swarm central control system needs sufficient communication channels to synchronize the data of each drone in the swarm, and a powerful system for encrypting and decrypting transmitted data to avoid interception and false information impacts.

2. With the information destruction of the control center, all drone systems disrupt the synchronization of the assigned tasks, since a swarm of drones controlled by one drone system performs only the tasks assigned from the main system.

3. In case of a cyber-attack or sabotage, a swarm controlled centrally and remotely from one place disrupts communication with the center and other drones, since the AI of a single drone in a swarm can only influence its own behavior, and does not have the function of transmitting information to other drones in the group.

Particular attention here can be paid specifically to armed drones since they perform combat missions. The advantage of centralized collective drone control can be called the speed of completing tasks and ensuring the effectiveness of a sudden strike on the enemy, and this in turn is an example of military tactics during combat operations.

A drone system built on the basis of the swarm algorithm due to the lack of communication channels has the highest viability, and, as a result, a high percentage of task completion. A minimum load of operators regardless of the number of drones can be considered another advantage of a drone swarm controlled by means of centralized control.

The disadvantage of this UAV control method is the complexity of the algorithms for controlling the control element and transmitting data, which can lead to a disruption in the service of the control system during sabotage intervention or the transmission of false information.

Moreover, the information and communication interaction of a drone in a group has a high level of vulnerability. In order to consider the disadvantages and the means, of using them to decipher the swarm, it is necessary to consider the general model for transmitting information to devices that are controlled via the centralized control system.

To achieve the goal of this study, the author sets the task of establishing the presence of disinformation by the enemy of the UAV, which is controlled remotely, and performs a combat mission in a group without its direct participation, since the fact of sabotage against one drone can provoke a disruption in the operation of the entire drone group, and, consequently, can cause losses and failure to achieve the goal. Therefore, the author assumes that information and communication interaction in a group of drones, without the direct participation of operators, is vulnerable when the drone perceives false information. To analyze in more detail the information and communication interaction of the UAV, the external and internal factors that affect the efficiency of the control system are considered.

Internal information and communication interactions of UAVs include the following elements:

- Sensors that collect information about changes in the area, weather conditions, and barriers;

- The processor, which takes part in the decoding of the received commands from the CGC;
- Engine and other technical elements that ensure the work of UAVs.

In order to fulfill tasks during the operation of a drone in a swarm, information is transmitted through internal information and communication channels. For example, information about coordinates, targets, the roll and pitch angles, area, the technical condition of the drone, a command to adjust the position in space, the location of the drone in relation to other drones in the group, the state of the drone and the command for combat missions.

The external information and communication interaction of UAVs consists in the exchange of information about their groups of drones and other groups of drones, about the location, changes in combat missions, losses, technical conditions and other data that ensure efficient distribution of tasks in real time.

Let's simulate the operation of a group of drones of the AnyLogic simulator (Fig. 1).

The swarm is represented in a 10 x 10 square cells, consisting of 5 UAVs. Each UAV has its own cell, and identification number from 1 to 5.

The goal of the group is to complete 10 tasks in the form of moving the "flags" to the zone, schematically indicated in gray in Fig. 1a. In order to fulfill the assigned tasks, the control center conducts centralized swarm management, distributing common tasks for each drone.

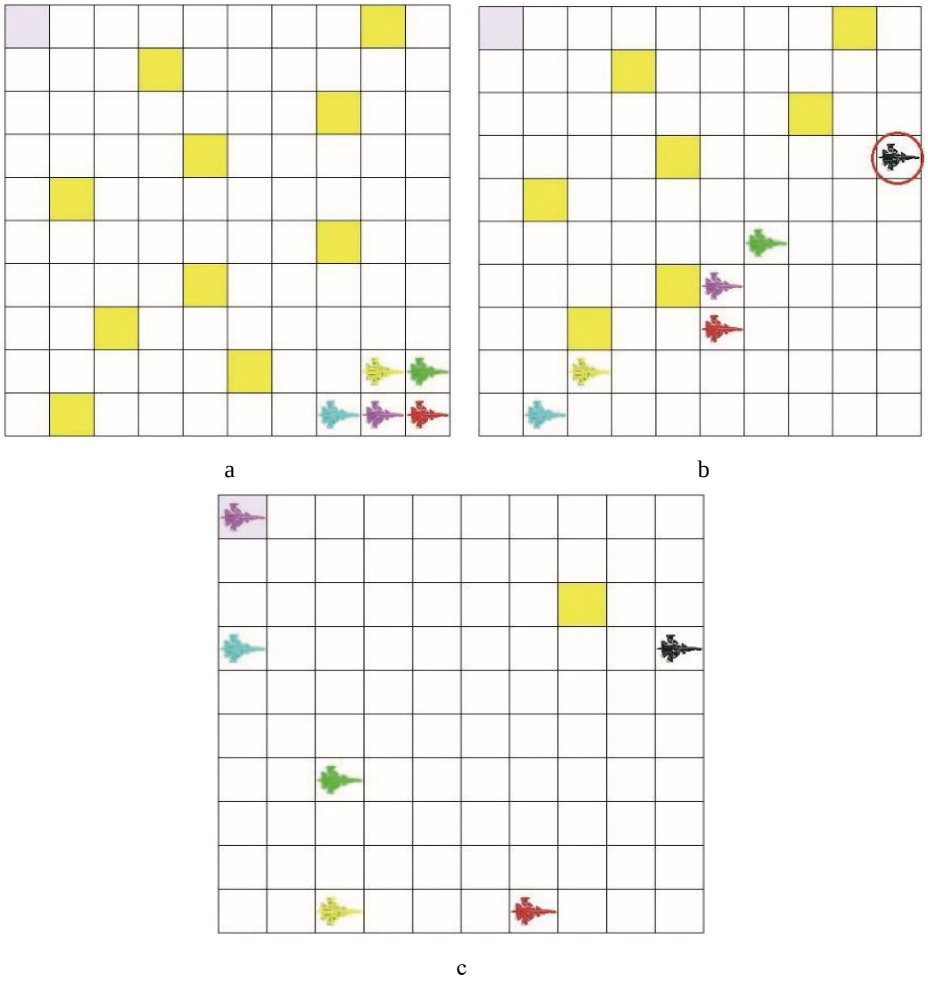

Fig. 1. Disruption in the operation of a group of unmanned aerial vehicles: group at the start of functioning (a); introduction of a false agent into a functioning group (b); disruption in the operation of the group (c)

A drone receives a task to perform if it is free from other tasks and is located closer than others drones to the system control center.

Tasks have a serial number and may have the status “failed” when data is accepted and not executed. Also, the task is considered failed if one of the UAVs does not accept it. Only the command executed by all drones gets the status of the task in progress. The status of the «completed» task is received only by those commands that are completed by all drones in the swarm.

To experimentally prove the vulnerability of the information and communication security of a group of drones, a drone, which will create conflict situations in the swarm by not accomplishing the task is launched. Since the vulnerability of swarm drones lies in their inability to influence other drones, and they are only capable of performing central control tasks, the swarm becomes disoriented and does not perform the task supplied by the central control system. The launched drone, which had false information about not completing the assigned tasks, provoked the entire swarm to fail to complete the assigned tasks.

Conclusion

The theoretical research is aimed at analyzing the security of data transmitted to UAVs in order to misinform and disrupt the combat mission performed remotely, without the direct involvement of operators. A theoretical analysis of scientific research on the chosen topic was carried out, namely, an analysis of the security of data transmitted to UAVs, for misinformation and disruption of the combat mission conducted in a group without the direct participation of an operator. The disadvantages of controlling swarms of drones by a single control center are analyzed. It has been established that external and internal data exchange can expose all elements of the system and information to false information since a drone controlled by one center cannot detect violations of the behavior of other drones in its group. An experiment in which the built-in drone accepted the task but did not complete it, and therefore the task was not completed by the entire swarm was conducted.

The conclusion of the research paper is that cryptographic methods cannot protect the drone from hidden hacker influences, sabotage, and cyber-attacks on data, so it is necessary to develop new methods to counter external influences with the involvement of IT specialists, linguists, and experts in the field of military security.

REFERENCES

1. Kirichenko V.V. Information security of communication channels with UAV electronics and control systems. 2015. H.3. P.23-27. Doi: 10.18372, 1990, 5548.45.9892.
2. Hooper M, Tian Y, Zhou R, et al. Securing commercial WiFi-UAVs from common secure attacks Proc. IEEE International Communications Conference. 2016. P.1213-1218, id: 10. 1109 MILCOM. 2 Kirichenko V.V. Information security of communication channels with UAV electronics and control systems. 2015. H.3. P.23-27. doi: 10.18372, 1990, 5548.45.9892.
3. Bayramov, A.A., Hashimov, E.G. Application SMART for small Unmanned Aircraft System of Systems. Chapter // Handbook of Research on Artificial Intelligence Applications in the Aviation and Aerospace Industries. IGI Global, PA, USA, 2019. Eds. T. Shmelova, Y.Sikirda, A.Sterenharz, 390 p. Chapter 8. Application SMART for Small Unmanned Aircraft System of Systems. pp.193-213.
4. Rivera E., Baikov R., Gu G. Analysis of randomness and cybersecurity. Texas, United States, 2014.
5. Chung T. H., Jones K. D., M. A. Day, M. M. Day, M. M. Day 50 in 2015: Swarm vs. Team UAV Live-Fly Contest at the postgraduate school on the Volga. AUWSI, 2013, p. 1792-1811.
6. Hashimov, E.G., Khudeynatov E.K. Evaluation of the effectiveness of the application of UAV systems in modern wars // - Baku: Military knowledge, - 2022. No. 1 (January-March), - p. 11-17.Javaid A.Y. Cyber security analytics and testing of an attack on an unauthorized aerial machine. PhD dissertation. University of Togliatti, 2015.016. 7895496.
7. Zikratov I.A., Zikratova T.V., Lebedev I.S., Gurtov A.V. Model of trust and reputation for objects of multi-agent robotic systems with decentralized control. Scientific and Technical Journal of Information Technology, Mechanics and Optics, 2014, no. 3.pp. 30-38.
8. Yakimenko O. A., Chung T. H. Using autonomous capabilities for systems with CORRUSER. Prospectus of the 28th Meeting of the International Union of Aeronautical Physics, ICAS 2012, 2012, p. 47–49.
9. Vatkin L., Li Kirichenko V.V.Information security of communication channels with UAV electronics and control systems. 2015. H.3. P.23-27. doi: 10.18372, 1990, 5548.45.9892.
10. Yang J. H., Kapolka M., Chung T. H. Autonomy in combat with the MUT command during a joint assault. Scientific and technical technologies and applications for robots, 2012, p. 561-5569. doi: 10" 1007 978-3642-3737-4-9 54".
11. Sidorov V., N. V. K., Lam K. I., Salle M. F. B. M. Cyberthreat analysis of UAV transport management for the city airport of the International Conference on Air Transportation. 2017.

Received (Надійшла) 13.02.2023
Accepted for publication (Прийнята до друку) 26.04.2023

Теоретичний аналіз рівня безпеки зв'язку БПЛА у складі групи виконання бойового завдання

П. А. Нагієва

Анотація. Актуальність дослідження полягає в питанні інформаційного впливу на ШІ безпілотника та його уразливості для здійснення противником диверсійних дій у локальних військових конфліктах. У статті проведено теоретичний аналіз захисту інформації, що передається групі БПЛА, з метою встановлення вразливості БПЛА до неправдивих даних та подальших організаційних дій, які можуть запобігти диверсійним діям противника та його союзників, а також аналізує ситуації, коли літальний апарат дезінформований, що в свою чергу тягне за собою невиконання завдання всією групою дронів. **Предметом та метою дослідження** є встановлення факту дезінформації противником БПЛА, що керується дистанційно та виконує бойове завдання у складі групи без безпосередньої участі оператора. У процесі моделювання ситуації були проведені теоретичні аналізи поведінки БПЛА, оскільки штучний інтелект в одному літальному апаратові здатний лише впливати на його поведінку і не в змозі при впливі неправдивої інформації встановити факт неправдивої дії. втручання противника в іншу групу безпілотників у ході бойових дій та попередження інших елементів системи у своїй групі. **Методами дослідження** є теоретичний аналіз комунікативної взаємодії рою дронів на основі вивчення дослідження алгоритмів операторського керування. **Отримані результати та висновок:** зашифрована неправдива інформація, що передається з метою дезорієнтації БПЛА, не може бути заздалегідь виявлена класичним підходом до запобігання кібератакам. У зв'язку з цим проблема інформаційної безпеки ШІ безпілотників залишається актуальною та потребує подальших комплексних теоретичних і практичних досліджень із залученням ІТ-спеціалістів, лінгвістів, інженерів, військових фахівців.

Ключові слова: безпілотний літальний апарат, група безпілотних літальних апаратів, штучний інтелект, інформаційна безпека, передача даних.