UDC 004.056:004.9:629.735/621.398

Simulation of UAV networks on the battlefield, taking into account cyber-physical influences that affect availability

Oleksii Novikov[1], Iryna Stopochkina[2], Andrii Voitsekhovskyi[3], Mykola Ilin[4], Mykola Ovcharuk[5]

[1,2,3,4,5] *National Technical University of Ukraine"Igor Sikorsky Kyiv Polytechnic Institute", Institute of Physics and Technology, 37, Prosp. Peremohy, Kyiv, 03056, Ukraine*

Abstract

The paper considers the types of countering means for unmanned aerial vehicles and the enemy's electronic warfare equipment used during the war in Ukraine. The types of cyber-physical influences that can be used to disrupt the availability of the network of unmanned aerial vehicles are addressed. The problem is also considered from the point of view of cybersecurity, taking into account possible harmful effects on the network of smart devices. Models based on complex networks, cellular automata and Petri nets are proposed, which allow solving the problem of optimizing the location of devices taking into account the set goal and countering cyber-physical attacks on availability and integrity. The proposed models differ from existing ones taking into account the conditions on the battlefield. A computational experiment has been performed that allows us to visualize the disposition of aircraft depending on the surrounding conditions on the battlefield. The results of the work can be used to develop a strategy for implementing operations of various types on the battlefield using UAVs.

Keywords: UAV, Cybersecurity, Cyber-Physical systems, Availability, Critical infrastructure simulation

Introduction

The use of UAVs in various areas of human activity is becoming increasingly widespread. Among such areas are industry and industrial process control [1], delivery of goods, monitoring of various kinds, and other tasks [2]. During the full-scale invasion of Ukraine, it became clear that the advantage in the field of unmanned aerial vehicles plays a decisive role in the struggle of the parties [3].

Existing research in the field of drones takes into account restrictions on their movement and communication, the type of networks, and other factors.

In particular, in the works [4-6], models in the form of cellular automata for pathfinding in the case of mobile robots are considered. The same principles can be used in the modeling of UAVs, this issue is discussed in the work [7]. Other aspects of modeling using cellular automata, presented in [8], suggest that a model in the form of a cellular automaton, with some restrictions, can be applied to modeling the behavior of UAVs and monitoring them.

Another approach to modeling UAV swarms is based on the apparatus of complex networks [9,10]. The work [10] considers cascading effects in networks that represent the communication environment of UAVs. The issue of optimizing complex networks is considered in the works [11,12], which makes it possible to apply the same approaches to UAV networks. The physical aspects of UAV motion, in particular those related to trajectory determination, are described in [13].

The apparatus of Petri nets can be useful in modeling the behavior of drones, as evidenced by the works [14,15]. Such models can be used to solve a variety of problems, including network performance optimization [16], security assessment [17], and drone cluster behavior modeling [18].

The field of drone research is well defined, as evidenced by the existence of frameworks such as [19].

However, the proposed works are applicable to the study of the use of drones for peaceful purposes. The conditions and nature of the use of UAVs in a military context, depending on the specifics of military operations during a particular war, were considered from the perspective of technical components [20], methods of conducting military operations [21], methods of physical counteraction to enemy attacks [22]. In particular, among the widely used ones are: multirotor UAVs (serve for reconnaissance, artillery correction, assault support, IED delivery, cargo delivery, remote mining, special operations (damaged drone evacuation, kamikaze missions, fire strikes); FPV drones (serve for ground strike drones, anti-aircraft missions); fixed wing drones (serve for long-range reconnaissance, kamikaze missions) [23-25].

The development of mathematical tools from the perspective of modeling networks of unmanned aerial vehicles, taking into account the capabilities of the enemy on the battlefield, as well as limitations in the form of cyber-physical attacks of the enemy, currently remains an relevant task.

This work proposes new models that can be used to model the behavior of the UAV network from the perspective of various tasks:

1) the task of optimizing the location of the UAV, taking into account the location of the target and the enemy's means of carrying out cyber-physical attacks.

2) the task of modeling the development of events during the spread of malicious cybernetic influences (malware) introduced by the enemy through the network.

3) the task of increasing the bandwidth of the communication network and the availability of individual devices, taking into account the terrain and the potential location of cyber-physical means of disruption of accessibility (communication disruptions) used by the enemy.

1. Overview of enemy devices used on the battlefield to organize cyber-physical attacks of availability violation

This section provides an overview of the enemy's technical means, based on open source data. The overview data provides factual information about the magnitude of the ranges of action, the mode of action of the devices, which must be taken into account when modeling.

1.1. Means of introducing cyber- physical interference

Let us review the most popular electronic warfare means of russian invadors. The results are given in Table 1, opensource information is used [26].

Table 1
Types of adversary electronic warfare

Electronic warfare ID	Suppression frequencies	Source power (W), suppres-sion range (km)
R-330Zh "Zhytel"	800 ... 960; 1227.6; 1575.42; 1500 ... 1700 and 1700 ... 1900 MHz, GPS, GSM, Inmarsat, Iridium mobile satellite suppression.	1000 W
"SHYPOVNY K-AERO"	25-100; 400-500; 800-925; 2400-2485 MHz.	0,1 km
RP-377UVM1 «LESOCHEK»	MHz – 20-80; 100-130; 120-197, 150-408, 386-1020.	20 W
LPD-801 anti-drone gun	2400-2483,5; 5725-5825; 1575- ., 1602- .	10;5;4;4 – accordingly to the frequency subrange
EW and "POLE-21" UAV	GPS/Galileo/GLONASS/BeiDou,	80W, 25 km
R-330 BMW	25 – 960 MHz	

EW complex "Sylok-01" UAV	390-490 MHz;
	870-950 MHz;
	1200-1300 MHz;
	1550-1600 MHz;
	2200-2500 MHz;
	4900-5900 MHz
		50W, 4 km

R-934UM	100-400 MHz	1000 W

Electronic warfare ID	Suppression frequencies	Source power (W), suppression range (km)
R-934UM “Altaiets-AM”	100-400 MHz 100-965 MHz	1000 W 200 W
«Leer-2»	30-2700 MHz	200-500 W
“Lorandyt”	137-174, 410-470,100-500 MHz	100 W
EW RB-341V “Leer-3”	880-915, 935-960, 1710-1785, 1805-1880 MHz.	3,5-6 km
EW “Krasukha”	2,9-3,2 HHz	250 km
EW RB-531B “Infauna”	25-2500	75W, 0,15 km
EW R-330, R-378A, R-378B “Mandat”	1,5 – 100 MHz	1000 W

The available data allow us to take into account in the model:

1) Types of UAVs vulnerable to this type of EW.
2) EW range.
3) Probability of EW hit (expert assessment should be taken into account here, depending on the power of this EW tool).
4) Type of hit (landing and/or disabling; disorientation).
5) Also, indirectly, we can take into account the accuracy of EW location according to intelligence data, depending on the power of the source. The more powerful the source, the more accurately it can be localized using radio reconnaissance. The accuracy of the location should be taken into account when setting the range..

When designing simulation software, facilities should be provided for entering appropriate constants and characteristics.

1.2. Cyber attacks on availability and integrity

The tools from the previous section can be considered as tools for disrupting accessibility by introducing interference, which ultimately affects the cybernetic functions of the device.

Additionally, cybersecurity attacks on UAVs can be used [27]. A threat model for drones is addressed in [28].

Attacks of this type may be relevant for distorting, intercepting intelligence data.

Also, dangerous attacks may be those that serve to intercept GPS coordinates or change them, intercept images and other intelligence information, replace signals to set the wrong direction, control UAVs via satellite [29].

Data on cyber attacks and the spread of malware by drone networks can be taken into account by modeling and comparing the delays that occur during the spread of malware and normal communication.

2. Cellular automata model

This section contains the prerequisites that a cellular automaton model should take into account and the potential capabilities of such a model.

2.1. Model description and restrictions

The aim of the modelling: imitation modelling of the signal distribution process in the network of UAV.

Automata type: dynamic colored probability automata (black, red, yellow, green), where the state color shows signal level (black means that signal is absent, red – the signal value is critically small, yellow – the signal level is in the middle range, green – the signal level is in maximum range).

The state of one automata cell should be described by following cortege: $\{S, P\}$, where S is the signal level, and P is position that consists of $\{x, y, z\}$ coordinates of UAV.

Neighbours: the maximal number of neighbours is N, where $N \neq 0$. For j-th UAV the set of neigbours will be denoted by O_j. The neighbour of i-UAV is j-UAV if $I(i,j) = 1$, where I is an adjacency matrix.

The initial automata state. It is given by an adjacency matrix I, $I(i,j) = 1$ if the connection between UAV i and j exists (non-black level) (and 0 otherwise). $I(i,j) = 1$ if

$$\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2 + (z_i - z_j)^2} \leq r,$$

where r is a minimal UAV sensitivity distance.

At the every step we reorganize the mesh of UAV's according to their trajectories of movement, so $\{x, y, z\}$ can change and adjacency matrix should be changed accordingly.

Also the position of command center is given: $\{x_c, y_c\}$ (in sense of the model it doesn't differ from ordinary UAV, but has bigger r and stable position).

The positions of radar warfare devices are given $\{x_k, y_k, z_k\}$, $k = 1 \dots M$. We consider these devices as such that can decrease signal level. The adjacency matrix for i-UAV and these devices: $R(i,r) = 1$ (rectangle matrix) if

$$\sqrt{(x_i - x_r)^2 + (y_i - y_r)^2 + (z_i - z_r)^2} \leq R_k,$$

where R_k is a radar warfare effectiveness distance. Also, we consider radar warfare devices neighbourhood for j-UAV: θ_j.

2.2. Model rules

The automata rules:

The automata rules:

1)If $\exists\, i \in O_j : S_i = \{green\}$ then $S_j\{red\ or\ yellow\ or\ green\} \to S_j\{green\}$ with probability P_g.

2)If $\exists\, i \in \theta_j$ then $S_j\{black\ or\ red\ or\ yellow\ or\ green\} \to S_j\{black\}$ with probability P_b.

Also there will be

3)additional rules for {yellow} → $\{red\}, \{green\} \to \{yellow\}\ or\ \{any\ color\} \to \{black\}$

depending on {x,y,z} and topology characteristics.

We'll take into account for rules 3) the following facts:

Inverse Square Law: Signal strength typically follows an inverse square law, where the signal power decreases with distance. This means that as UAV devices move farther apart, the signal strength diminishes rapidly, leading to higher signal degradation.

The inverse square law describes the relationship between signal strength and distance in a scenario where the signal spreads out uniformly in all directions from its source. The formula for the inverse square law is:

Signal Strength=Constant/Distance^2

Where Signal Strength is the strength or intensity of the signal at a certain distance from the source. Constant is a proportionality constant that depends on various factors such as the power of the transmitter, characteristics of the medium through which the signal propagates, and the sensitivity of the receiver. Distance is the distance between the transmitter (source) and the receiver.

Obstacles and Interference: Signal degradation can also occur due to obstacles such as buildings, terrain features, or other UAVs, as well as interference from other wireless devices operating in the same frequency band. These factors can attenuate the signal and reduce its quality over distance.

Line-of-Sight vs. Non-Line-of-Sight: In scenarios where there is a clear line-of-sight between communicating devices, signal degradation may be lower compared to non-line-of-sight scenarios where signals must traverse obstacles or reflect off surfaces, leading to additional attenuation and multipath effects.

4)additional rule concerning different type radar warfare devices influence for signal level. Type 1: {yellow} → $\{red\}$, $\{green\} \to \{yellow\}$, {red}→ $\{black\}$;
type 2: {green, yellow, red, black} → $\{black\}$.

3. Petri net model

This section provides a description of a Petri net for modeling the status of devices in a UAV network.

3.1. Model description

The tokens that describe the state of one network device are signal levels. Three tokens mean the highest level, one – the critical (weakest) level. To model the network behavior, such a model should be applied to each UAV.

The starting signal level corresponds to three markers that denote conditional signal levels.

Transitions from one state to another are shown by rectangles. Among them are:

1) Decrease/increase of the signal level with increase/decrease of the distance to the control center;

2) Decrease of the distance to the control center according to the control signal of the control center;
3) The influence of the terrain (taken into account using a topological height map and the location of the device), thus taking into account that the device must be in the "line-of-sight" with the drone-"hub", or the control center (Fig.1). We can use OpenDEM for landscape simulation.
4) Signal amplification if a drone-hub appears in the "line-of-sight" within the radius of action of this device, which relays the center's signals;
5) The impact of powerful electronic warfare means that completely disrupt the functionality of the UAV;
6) The impact of less powerful electronic warfare means that disorient the UAV for a while, however, after leaving the EW zone, the UAV's functionality is restored.

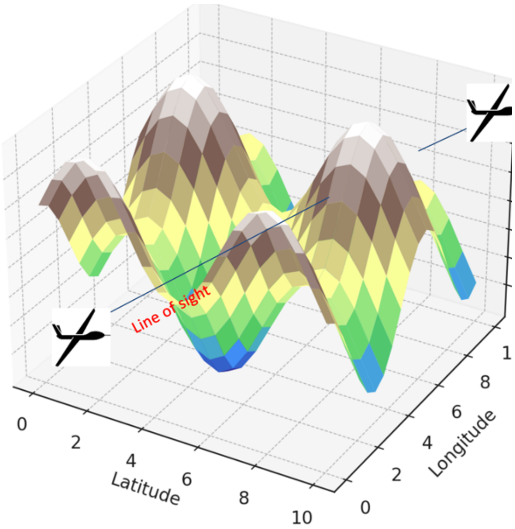


Figure 1: Line-of-sight is interrupted by landscape

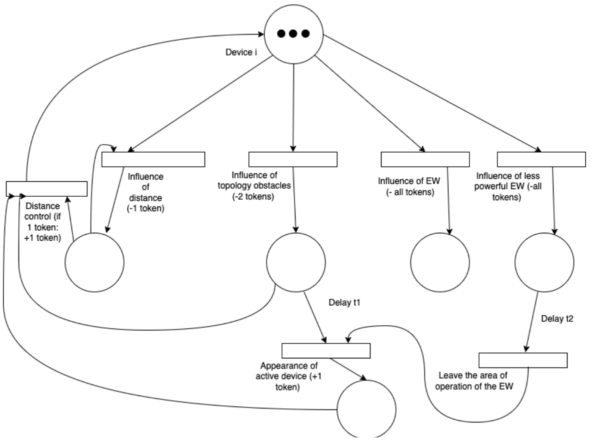

Device i
Influence of distance (-1 token)
Influence of topology obstacles (-2 tokens)
Influence of EW (- all tokens)
Influence of less powerful EW (-all tokens)
Distance control (if 1 token: +1 token)
Delay t1
Delay t2
Appearance of active device (+1 token)
Leave the area of operation of the EW

Figure 2: Proposed Petri net structure

3.2. Potential purpose of the model

The model takes into account topological obstacles, and the effects of various types of electronic warfare. The model takes into account delays, and can be used to predict the speed of interactions under various conditions.

4. Models based on complex networks

The section provides information on the characteristics of complex networks and the formulation of the optimization problem.

4.1. Model description and restrictions

The aim of the modelling: we consider the UAV network as a complex network, and should calculate the set of characteristics that can help us to conclude about its stability and additional features.

In addition to rules 1)-6) from the description of the model in the form of a Petri net, when modeling a complex network, we take into account the types of control messages - intended for a specific UAV and intended for all network devices.

When modeling, we assume that all drones that are in the control center's range are trying to connect to it. However, signal transmission between drones in this area is also provided. For example, if the signal level directly with the control center is weaker than the signal level received from the drone-hub, then the latter is given priority.

The difference between the rules of operation of a complex network and a cellular automata lies in the deterministic principle of applying the rules, while in a cellular automata certain probabilities are provided. Also, changes in the states of the nodes of a complex network occur in stages, while the recalculation of the states of all "cells" of a cellular automaton occurs instantly.

Thus, a complex network makes it possible to take into account certain delays inherent in the transmission process and the effects of cascading interactions.

4.2. Model rules

Let us list the parameters that are essential when modeling a complex network.

The shortest path (geodesic line) between any two network nodes is the length of the shortest path between these nodes. When considering an unweighted network, when the conditional weight of each edge is equal to one, the geodesic line is the path from one node to another with the smallest number of steps. Using this parameter can make it possible to build the signal level depending on the distance to the control center or drone-hub and to model delays.

The network diameter is the maximum distance between two network vertices. This parameter can make it possible to determine the territorial scope of the operation.

The distribution of nodes by the number of connections (degree distribution) is a numerical characteristic of a complex network that indicates the probability $P(q)$ that a randomly selected vertex of the network will have degree q. For a directed network, the coefficients for the input and output degrees of the node are calculated separately. We can calculate this characteristic dynamically, determining, for example, the concentration of drones around the target, which is accompanied by an increase in the degree of each node.

Clustering is a local characteristic of the network that characterizes the degree of interconnectedness of the nearest neighbors of the selected node. Usually, real complex networks have the following property: if any two nodes are adjacent, and one of them is also adjacent to some third node, then the first node will also be adjacent to the last one. Clustering can help determine the stability of the network under the influence of terrain heights, or the failure of individual devices.

Let us give mathematical expression. If node j has q_j nearest neighbors with the number of t_j connections between them, then the local clustering coefficient is calculated according to the following formula:

$$C_j(q_j) = \frac{t_j}{q_j(q_j-1)/\,2} \text{ ,}$$

The value of the numerator in this sense is the total number of triangles (cycles of length 3) associated with vertex j, and the denominator is the total possible number of such triangles in the network.

The adjacency matrix is a matrix that unambiguously defines the structure of the neighborhood in the network. For a network with the number of nodes N, the adjacency matrix will have the dimension $N \times N$. The adjacency matrix is filled in as follows - if connection goes from node i to node j, then there is one at the intersection of the i-th row and the j-th column. Otherwise, if there is no connection from node i to node j, then it is zero. We assume that matrix can be asymmetrical in general case. This is due to the fact that some devices can only be receivers of the signal, but cannot transmit it to others.

Node load (a measure of centrality, or betweenness centrality) is a coefficient that, in a general sense, characterizes the importance of a given node for the network, and is described using the value of the number of shortest paths between some nodes, for which these paths pass through the selected node. This coefficient is described with the help of quantitative calculations of the shortest paths in the network associated with the chosen one, and in a general sense it can be understood as an indicator of how important this or that node is for the entire network. The load factor is calculated for each network node separately according to the following formula:

$$b(i) = \sum_{st} \frac{\sigma_{st}(i)}{\sigma_{st}},$$

where i is the index of current net node,
$\sigma_{st}(i)$ is the number of shortest paths between nodes s and t that pass through the selected node i,
σ_{st} is the total number of shortest paths between nodes s and t in the addressed network.

Coefficient of network connectivity C:

$$C = \frac{N_{after}}{N},$$

where N – the general number of nodes in initial network M, and N_{after} – the number of nodes in the most connected component of the resulting network $M`$, which is formed after deletion of some nodes.

In terms of UAV network, we assume that path between nodes (UAVs) exists if one of UAVs is in the operation radius of another, that means they are free to establish connection and data transfer.

Compared to the degree characteristic of a node (the number of edges with which a node is connected), which rather gives information about an individual node, load factors in some sense reflect the overall topology of the network [30].

When nodes are randomly removed from a graph, there is typically a critical threshold—determined by the ratio of removed nodes to the total number of nodes in the network—beyond which the network fragments into isolated clusters. In scale-free networks, this critical threshold is absent. Research indicates that even if a substantial portion of the nodes is removed, the remaining nodes are still highly likely to form a connected cluster.

In contrast, other types of networks may have certain critical nodes whose removal or failure could cause significant disruption to the entire network.

The issue of network stability (the percolation problem) under accidental damage is closely tied to factors like radar warfare devices and other external influences. The rate at which negative effects spread depends on the network's topology, the initial nodes affected, the number of their connections, and other node-specific characteristics. For instance, factors such as a large distance between connected nodes, a low total number of connections for the selected nodes, or low centrality coefficients of these nodes can significantly impact the percolation process.

4.3. Network optimization

Our main goal to optimize network, having some goals. Let us list what we should consider.

In our criteria of network optimization we should take into account the following aspects. We should be sure that maximal number of UAVs remains connected to the network, either directly or through UAV hubs, for maximal information flow. Also we have to maximize the number of UAVs within communication range or ensure a robust relay mechanism.

More precisely, we should maintain a minimum signal strength threshold to avoid UAVs disappearing from the network. We can plan position UAV-hubs strategically to strengthen weak signals and extend the effective range of isolated UAVs. And, we should supply minimization of lost control messages from the control center to UAVs. It can be reached by ensuring the critical UAV-hubs between the control center and outlying UAVs have high reliability and protection, taking into account cybersecurity means also.

Another important issue is to supply resilience of the network to Electronic Warfare (EW). We can distribute control dependencies across multiple UAV-hubs to reduce single points of failure. The repositioning of UAVs to avoid known positions of EW also should be made. We should introduce redundancy in communication pathways to maintain network integrity if certain UAVs are compromised.

In real situation, we should take into account energy efficiency of the network. It means, we should optimize UAV positions to reduce energy consumption caused by excessive distance or reliance on signal amplification. This task is also related with limitations for unnecessary UAV movements while maintaining network coverage and connectivity.

When we address the UAVs use for reconnaissance, we should maximize the geographic area monitored by the UAVs while preserving connectivity to the control center. Also, we should ensure critical regions have overlapping coverage to account for potential UAV losses. When we address the UAVs use for hitting the target – the criteria should be changed, taking into account target coordinates for combat UAVs.

Also, we can take into account complex network characteristics, such as centrality. E.g., we prioritize protection and reinforcement of UAVs with high centrality (betweenness or closeness centrality) as their loss could critically impact network performance.

To make our network stable, we should balance the network load to prevent premature depletion of UAV energy resources. Also, in practical case, we can rotate UAV roles (e.g., hub vs. end node) to avoid energy depletion.

By combining these criteria into an optimization framework we come to the problem of multi-criteria optimization.

To formulate the optimality criteria in the form of certain expression, let us define objective function in form:

$$J = w_1(N - |A|)^2 + w_2 \sum_{i\in \mathrm{T}}[(x - x_t)^2 + (y - y_t)^2 + (z - z_t)^2] \rightarrow min;$$

where N – the general number of UAVs, A is the set of “alive” UAVs connected to the network and control center, $|A|$ is the number of elements in the set, so, the first term of the criteria minimizes the number of UAVs that are “not alive” (i. e. disconnected or removed from the network).

$T \subseteq A$ is a subset of UAVs required to reach target coordinates $(x_t,\ y_t, z_t)$,

w_1, w_2 are weight factors for “alive” UAVs and movement to the target coordinates, respectively. The second term measures the squared Euclidean distance of UAVs in the subset T from the target coordinates (x_t, y_t, z_t).

Let us formulate other conditions as constraints.

Connectivity condition is

$$S_i > 0\ \forall i \in A,$$

where S_i is signal level (signal strength).

Signal strength condition is given by

$$S_i = S_0 - \alpha d_{ic} + \beta \sum_{j \in A, j \neq i} f(d_{ij}),$$

where $d_{ij}$is distance between UAV i and UAV j,
r is maximum communication range of UAV,
$f(d_{ij})$ is signal contribution from neighboring UAV (e.g., $f(d_{ij}) = \exp(-d_{ij})$ or $f(d_{ij}) = 0$ if $d_{ij} > r$),
α is signal attenuation factor with distance d_{ic} to the control center,
β is amplification factor from UAV-hubs.

5. Simulation results and perspectives

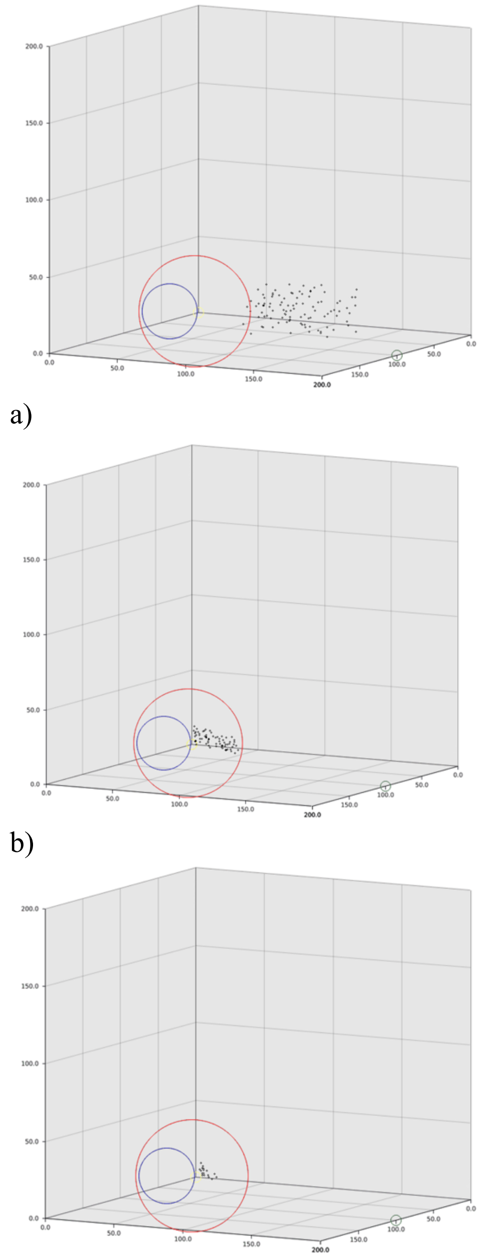
This section contains a description of the results of computer modeling, which allow us to assess the prospects for using the proposed models.

5.1. Simulation with taking into account the electronic warfare means

We realized practical experiment. For this purpose appropriate software was developed. It gives a possibility to assess drones behavior in different cases of availability attacks.

In these figures black dots depict drones. Green circle is operating area of the control center. Yellow circle is the drone destination area. (assume that the drone exploded upon contact with the target). The red circle - zone of EW that suppresses all connection. When crossing it, the drone no longer receives data about its geolocation and moves horizontally in the same horizontal direction in which it moved before entering the zone.

Blue circle is zone of action of the EW, which suppresses the control connection. When crossing it, the connection with the drone is lost, that is, the drone is removed from the network.



a)

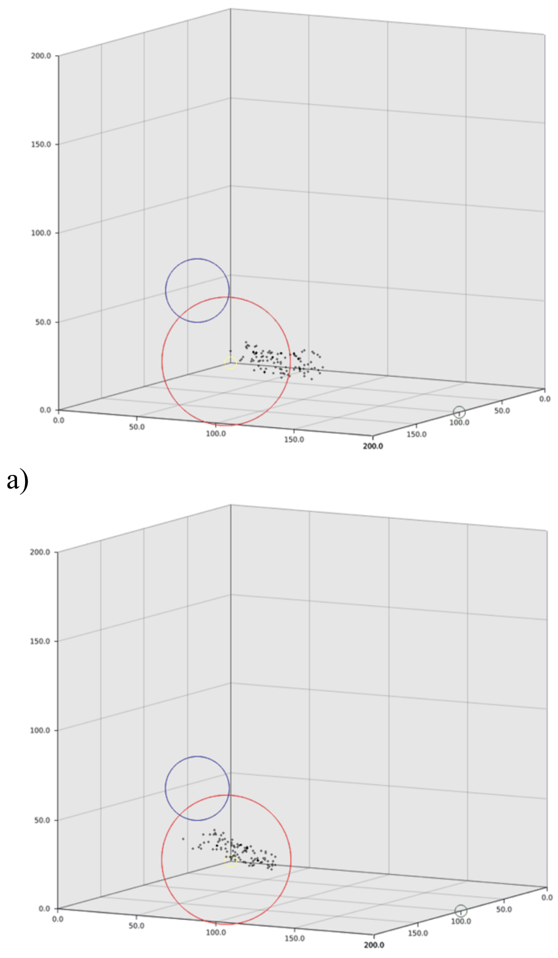
b)

c)

Figure 3. Full availability control by electronic warfare

Figure 3 shows being in the range of electronic warfare, which suppresses all communication. The drone is completely lost for control for control center and is not available for signals from hub drones. Fig.3a shows the beginning of drones movement, fig.3b shows entering the geolocation signal suppression zone and approaching the zone of complete signal suppression. Fig 3c) shows disappearance of drones from the network due to complete loss of control over them, possibly it leads to physical destroyment.

Drones that fall into the red EW zone are disoriented (fig. 3a)). But still exists probability that drone can leave the zone and return to normal functioning.



a)

b)

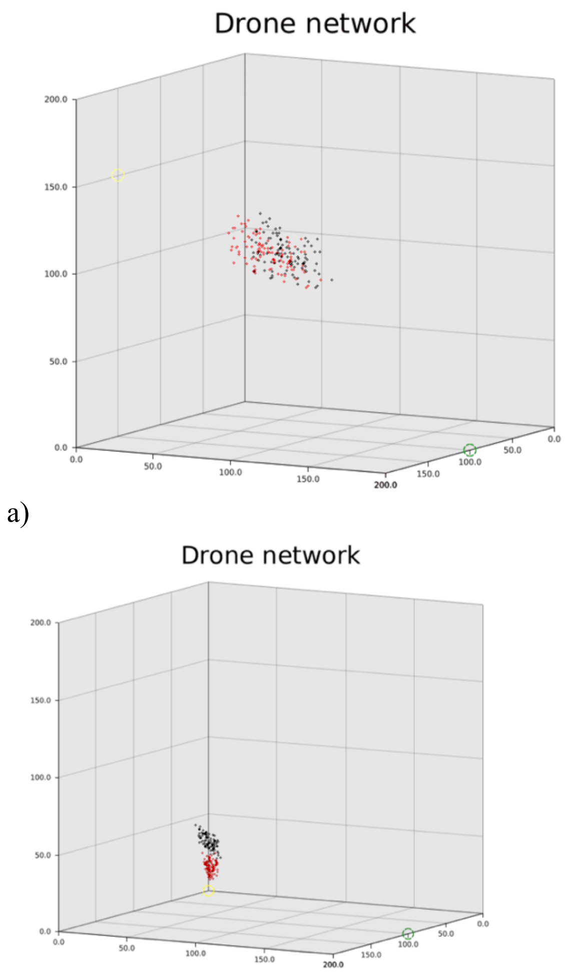
Figure 3. Partial availability control by electronic warfare

Once in the EW area, they fly until they accidentally fly out of this zone, or until their energy resource is depleted. It is illustrated in fig.3b)

5.2. Simulation with taking into account the possible delays

The next kind of experiments is devoted to simulation in conditions of delays. It can be useful for investigation the normal patterns and patterns, when malware introduces some delays in data transfer.

Red dots show normal movement of drones, and black ones show drones which react on commands with delay (fig.3a). The difference in behavior is very noticeable when changing the trajectory of movement (fig.4b)).



a)

b)

Figure 3. Delays in drones movement that partially affect availability

Conclusion

The results obtained in this work are the foundation for further research. In particular, the next steps should be to solve the problems of optimizing drone networks, and the problem of modeling drone networks under conditions of delays caused by various types of harmful cyber-physical influences.

The practical significance of the obtained results lies in providing the possibility of strategic planning of operations using drones, taking into account the topology of the terrain, communication delays, changes in the signal level, means of violating accessibility implemented by the attacker, and other factors.

Acknowledgements

The research presented in this paper was supported by the Impress-U grant: «Towards Networked Airborne Computing in Uncertain Airspace: A Control and Networking Facilitated Distributed Computing Framework».

The authors express their gratitude to the student of the Educational and Scientific Physics and Technology Institute Anton Tyshchenko for his active assistance in implementing computer experiments.

References

[1] D. Mourtzis, J. Angelopoulos, N. Panopoulos, UAVs for Industrial Applications: Identifying Challenges and Opportunities from the Implementation Point of View, Procedia Manufacturing, Vol. 55, 2021, 183-190. doi:10.1016/j.promfg.2021.10.026.

[2] J. Xie, L. R. G. Carrillo, L. Jin, An integrated traveling salesman and coverage path planning problem for unmanned aircraft systems, IEEE control systems letters, Vol. 3, No. 1, 2019, 67-72. doi: 10.1109/LCSYS.2018.2851661.

[3] A. Kobalia, M. Light, UAVs in Ukraine and Their Future in Warfare, 2024. URL: https://www.internationalaffairs.org.au/australianoutlook/uavs-in-ukraine-and-their-future-in-warfare/#:~:text=UAVs%20have%20also%20become%20a,provoke%20the%20enemy%20into%20action.

[4] U.A. Syed, F. Kunwar, Cellular Automata Based Real-Time Path-Planning for Mobile Robots, International Journal of Advanced Robotic Systems, 2014, 1-15. doi: 10.5772/58544.

[5] K.Ioannidis, G. Ch.Sirakoulis, I. Andreadis, A Path Planning Method Based on Cellular Automata for Cooperative Robots, Applied Artificial Intelligence, Volume 25, Issue 8, 721 - 745, doi: 10.1080/08839514.2011.606767.

[6] C. Behring, M. Bracho, M. Castro, J.A. Moreno. An Algorithm for Robot Path Planning with Cellular Automata. In: Bandini, S., Worsch, T. (eds) Theory and Practical Issues on Cellular Automata. Springer, London, 2001. doi: 10.1007/978-1-4471-0709-5_2.

[7] Z. Song, H. Zhang, X. Zhang and F. Zhang, "Unmanned Aerial Vehicle Coverage Path Planning Algorithm Based on Cellular Automata, 2019 15th International Conference on Computational Intelligence and Security (CIS), Macao, China, 2019, pp. 123-126. doi: 10.1109/CIS.2019.00034.

[8] Zakharchenko I., Tristan A., Chornogor N., Berdnik P., Kalashnyk G., Timochko A., Zalevskii A., Dmitriiev, Modeling of Object Monitoring Using 3D Cellular Automata, Problemele energeticii regionale, 4 (56), 2022, 61-73. doi: 10.52254/1857-0070.2022.4-56.06 .

[9] J. Zhou, K Liu, Y.Lu, L.Chen. Complex network–based pinning control of drone swarm, IFAC-PapersOnLine 55(3), 2022, 207-212. doi: 10.1016/j.ifacol.2022.05.036.

[10] B.Feng, L.Zhou, Z.Zhang. Study on Cascading Failure and Elasticity of UAV Swarm Communication Network, Mathematical Problems in Engineering, 2022, 6166849, 14. doi: 10.1155/2022/6166849.

[11] R.Ferrer-i-Cancho, R.Sole. Optimization in Complex Networks. In: Pastor-Satorras, R., Rubi, M., Diaz-Guilera, A. (eds) Statistical Mechanics of Complex Networks. Lecture Notes in Physics, Vol. 625. Springer, Berlin, Heidelberg. doi: 10.1007/978-3-540-44943-0_7.

[12] M. T. Thai, P. M. Pardalos, Handbook of Optimization in Complex Networks, Optimization and Its Applications, Springer, ed. 1, number 978-1-4614-0754-6. doi:10.1007/978-1-4614-0754-6.

[13] J. Xie, Y.Wan, B. Wang, S. Fu, K. Lu, J.H. Kim, A comprehensive 3-dimensional random mobility modeling framework for airborne networks, IEEE Access, Vol. 6, 2018, 22849-22862. doi: 10.1109/ACCESS.2018.2819600.

[14] A. Fedorova, V. Beliautsou and A. Zimmermann. Colored Petri Net Modelling and Evaluation of Drone Inspection Methods for Distribution Networks, Sensors, 22(9), 2022, 3418. doi:10.3390/s22093418.

[15] D. Xu, P. Borse, K. Altenburg, K. Nygard. A Petri Net Simulator for Self-organizing Systems., Proceedings of the 5th WSEAS Int. Conf. on Artificial Intelligence, Knowledge Engineering and Data Bases, Madrid, Spain, February 15-17, 2006, pp.31-35. URL: https://www.researchgate.net/publication/23

4805596_A_Petri_net_simulator_for_self-organizing_systems.

[16] W. Shi, Z. He, C. Gu, N. Ran, and Z. Ma, Performance Optimization for a Class of Petri Nets, Sensors 2023, 23(3), 1447. doi: 10.3390/s23031447.

[17] P. Gonçalves, J. Sobral, L.A. Ferreira, Unmanned aerial vehicle safety assessment modelling through petri Nets, Reliability Engineering & System Safety, Vol. 167, 2017, 383-393, https://doi.org/10.1016/j.ress.2017.06.021.

[18] X. Wang, Y. Guo, N. Lu and P. He, UAV Cluster Behavior Modeling Based on Spatial-Temporal Hybrid Petri Net, Appl. Sci. 13(2), 2023, 762; doi: 10.3390/app13020762.

[19] IEEE Std 1936.1-2021; IEEE Standard for Drone Applications Framework. The Institute of Electrical and Electronics Engineers,Inc.: New York, NY, USA, 2021, pp. 1–28. doi: 10.1109/IEEESTD.2021.9652498.

[20] Z. Malinowski, The role of unmanned aerial vehicle in the formation of a secure military supply chain, Security and Defence Quarterly, 12(3), 2016, 19-45. doi: 10.35467/sdq/103235.

[21] I. Shovkoshytnyi, O. Vasylenko, The problematic issues of swarming use of striking unmanned aerial vehicles, Modern Information Technologies in the Sphere of Security and Defence, 2023.

[22] How the Defense Forces can counter enemy electronic warfare (EW) capabilities (in Ukrainian). URL: https://armyinform.com.ua/2023/11/15/yak-sylam-oborony-protystoyaty-zasobam-reb-protyvnyka-dumka-eksperta/.

[23] About the connection from Serhii Flash (in Ukrainian). URL: https://t.me/serhii_flash .

[24] US Infantryman (In Ukrainian). URL: https://t.me/usinfantryman1/17820.

[25] Berlinska (in Ukrainian). URL: https://t.me/MariaBerlinska/ .

[26] Enemy electronic warfare means (in Ukrainian). URL: https://sprotyvg7.com.ua/lesson/zasobi-radioelektronnoi-borotbi-voroga .

[27] Zh. Wang, Y. Li, Sh. Wu, Yu. Zhou, L. Yang, Yu. Xu, T. Zhang, Q. Pan, A survey on cybersecurity attacks and defenses for unmanned aerial systems, Journal of Systems Architecture, Vol. 138, 2023. doi: 10.1016/j.sysarc.2023.102870 .

[28] A. Esquivel Morel, D. Kavzak Ufuktepe, R. Ignatowicz, A. Riddle, Ch. Qu, P. Calyam and K. Palaniappan, Enhancing Network-edge Connectivity and Computation Security in Drone Video Analytics, 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), Washington DC, DC, USA, 2020, pp. 1-12. doi: 10.1109/AIPR50011.2020.9425341.

[29] G.E. M. Abro, S. Zulkifli, R.J Masood et al. Comprehensive Review of UAV Detection, Security, and Communication Advancements to Prevent Threats, Drones 2022, 6(10), 284. doi:10.3390/drones6100284.

[30] O. Novikov, G. Vedmedenko, I.Stopochkina, M.Ilin, Cyber attaks cascading effects simulation for Ukraine power grid, CEUR Workshop Proceedings, Vol. 3241, 2021, pp.23-35., URL: https://ceur-ws.org/Vol-3241/.