The Improved Algorithm for Reducing the UAV Swarm Radio Visibility

Leonid Hulianytskyi and Maksym Ogurtsov

V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine, Akademika Hlushkova Ave, 40, Kyiv, 03187, Ukraine

Abstract

This work presents the developed set of improved data transmission algorithms with adaptive signal power for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm, the purpose of which is to minimize the power levels of swarm members (UAVs) transmitters, and to optimize data transmission routes within the swarm Relevance of this research is high because of heavy losses, that UAVs facing during the surveillance and strike missions during a full-scale military combat.

The requirements to UnACs to ensure the possibility of the developed family of data transmission algorithms usage for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm are formulated. The data transmission with reduced signal power problem for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm was formulated as an optimization problem. The improved UAV swarm network initialization algorithm for data transmission and radio visibility reduction is developed. The improved algorithms that will support further operation of an UAV swarm for data transmission and radio visibility reduction during a mission are developed and practically tested. There were analyzed advantages and disadvantages of the improved algorithms compared to its previous version.

Keywords [1]

UAV, unmanned aerial vehicle, unmanned aerial complex, swarm, radio visibility

1. Introduction

During the execution of combat missions using unmanned aerial complexes (UnAC, usually containing one or a few UAVs, a ground control complex for an operator and any necessary additional means) on the combat line (and behind it), a whole set of measures aimed at preserving both the personnel and the UnAC components [1, 2, 3] must be carried out. They mostly depend on the UnAC type [4, 5, 6]. A full consideration of all these measures (including, for example, different locations of an operator and a transceiver antenna, position masking, etc.) is beyond the scope of this paper, but partially were analyzed in authors' previous works [7, 8, 9].

This work describes a certain number of measures developed to reduce the probability of losing a UAV swarm (whole or partially) during a combat mission. These measures should include cryptographic protection of information circulating between a UAV and its operator, ensuring privacy protection [8, 9] – but are not limited to cryptography [10]. Cryptographic protection aimed against the detection of an operator's position, the interception of the control over the UAV (access control means), against the sending of false data to an operator (spoofing), etc. [1, 9].

Relevance of this research is very high because of heavy losses, that UAVs facing during the surveillance and strike missions during a full-scale military combat. They are caused by the enemy's electronic reconnaissance means, followed by various strikes (means of electronic warfare, means of

Information Technology and Implementation (IT&I-2023), November 20-21, 2023, Kyiv, Ukraine
EMAIL: LeonHul.icyb@gmail.com (A. 1); maksymogurtsov@mail.com (A. 2)
ORCID: 0000-0002-1379-4132 (A. 1); 0000-0002-6167-5111 (A. 2)

physical damage, etc.). According to some sources these losses sometimes may be up to 60-80 percents per mission. Additionally similar tasks are currently under attention from scientists all over the world [11, 12, 13, 14]. The main proposed ways for solving this problem are:

- mixed-strategy Stackelberg Equilibrium, which is using finite and discretized power set in addition to the hierarchical Q-learning based power control algorithm [11]
- scalable specific emitter identification neural network with SNR-aware adaptive precision computation [12]
- successive convex approximation, based on Dinkelbach method and coordinates decent techniques, plus usage of the iterative power control algorithm [13]
- algorithm, making each UAV rotate relatively to the position of its neighbouring UAVs, in order to optimize its antenna radiation direction [14] (applicable only for stable relay positions).

The main reason, that limits application of the mentioned solutions (and other existing options as well) is great computational load on UAV's system (or even computations, made beforehand on the operator's side), requiring high-productivity hardware or lots of time to compute (or just a lot of resources) and therefore – greatly limiting application area of these solutions.

This work presents the developed set of improved data transmission algorithms with adaptive signal power for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm, the purpose of which is to minimize the power levels of swarm members (UAVs) transmitters, and to optimize data transmission routes within the swarm. Simulations provided on the basis of the V.M. Glushkov Institute of Cybernetics of the NAS of Ukraine hardware show that the suggested family of algorithms outperforms the results of the previously proposed works.

2. The main issues considered in this work

The main issues considered in this work are:

1. Formulation of requirements to UnACs to ensure the possibility of the developed family of data transmission algorithms usage for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm.
2. Formulation of the data transmission with reduced signal power problem for protection against radio-electronic warfare and reducing the radio visibility of a UAV swarm.
3. Development of the improved UAV swarm network initialization algorithm for data transmission and radio visibility reduction.
4. Development of the improved algorithms that will support further operation of an UAV swarm for data transmission and radio visibility reduction during a mission.
5. Analysis of advantages and disadvantages of the improved algorithms compared to its previous version.

3. Formulation of requirements to UnACs to ensure the possibility of the developed family of data transmission algorithms usage

During the work on the reducing the UAV swarm radio visibility, there were formulated the main requirements for the UAV swarm, which must be fulfilled to ensure the corresponding algorithms performance. Let's consider these requirements:

Requirements for wireless signal transmitters and receivers:

Since UAVs already have receivers and transmitters installed to establish communication with the operator (both to transmit control signals to the UAV and to transmit back service information (GPS coordinates, telemetry, battery charge, etc.) and photo/video signal), then by default they meet most of the requirements for ensuring the operation of the proposed family of algorithms. The communication system must have the ability to send high-frequency data packets (with a certain fixed interval) and at the same time receive data over the radio channel (operate in duplex mode).

The main requirement that must be met (and is met on most modern UAVs):

- Ability to programmatically control the signal power level transmitted from the UAV.

Without fulfilling this requirement, it is impossible to ensure the operation of the proposed algorithms. To ensure communication, it is recommended to use the frequency range of 2100 - 2400 MHz, OFDM modulation. It is desirable to use wide-band noise-like signals with support of the possibility to switch the frequency in case of aiming interference (signal jamming).

It is recommended to use the 860-930 MHz frequency range for telemetry transmission (additional channel). An additional requirement (optional) is the possibility of directional signal transmission (instead of the usual omnidirectional). It will make it possible to communicate with other elements of the swarm with a directional signal, which will allow to reduce the radio visibility of the swarm as a whole (and its individual elements), as well as to make it more difficult to jam the signals transmitted between the nodes of the swarm by electronic warfare means.

Of course, UAV should provide enough lifting power, which is different depending on the UAV type [5]. For wing-type UAVs this lift is given by the equation

$$L = 0.5\rho V^2 S C_L, \qquad (1)$$

where C_L is a coefficient that determines the ability of the wing of area S to deflect the airstream, ρ is the reciprocal of the air density kg/m2, and the square of the reciprocal of the airspeed V m/s. From this equation we may get the absolute minimum flight speed for the wing-type UAVs (allowing margin in speed or in lift coefficient), which will be equal to

$$V_{min} = \left(\frac{2L}{\rho S} C_{Lo.}\right)^{0.5}, \qquad (2)$$

where C_{Lo} (operating C_L) has been chosen to have a value of about 0.2 less than the C_L.max.

Usually, the standard wing section offers a C_L.max of about 1.2 for real-life UAVs (wing-typed) without flaps. Therefore, a value of 1.0 has been used as a basis value.

Equation (2) can be rewritten as:

$$V_{min} = (2w/\rho C_{Lo})^{0.5} \; or \; \left[\left(\frac{2}{\rho_0}\right)^{0.5} \left(\frac{w}{\sigma}\right)^{0.5}\right], \qquad (3)$$

where w is the aircraft wing loading in N/m2, ρ_0 is the air density at sea-level standard conditions and σ is the relative air density at altitude.

For the rotary-wing UAVs different formulas should be used to found out their lifting power and corresponding lift-induced drag. The UAV's velocity induced by its rotor in the hover is given by:

$$v_i = k_n (p/2\rho)^{0.5}, \qquad (4)$$

where k_n is a correction element for the efficiency of the UAVs lift distribution and the strength of the tip vortices generated by the rotor blades. Usually, they vary between 1.05 and 1.2, so we will use 1.1 value.

The induced power for this UAVs type is then given by $P_i = k_n \cdot T v_i$, where T is the thrust produced by the UAVs rotor [5].

Also, in the process of laboratory experiments, **the requirements for the hardware that will implement the formation of data packets according to the proposed algorithms were formulated**:

- Program memory (hard disk, flash memory, etc.): 256 kB or higher.
- RAM/SRAM: 8 kB or higher.
- EEPROM non-volatile memory: 4 kB or higher.
- Clock frequency of the processor: 16 MHz or higher.
- Number of processor cores: from 1.

Other factors also should be considered, especially UAVs aerodynamics N_R is given by the expression

$$N_R = \frac{vl}{\nu}, \qquad (5)$$

where v is the flow (air) speed; l is the characteristic length (e.g. wing chord) and υ is the kinematic viscosity of the fluid and has a value of 1.47 × 10−5 m2/s for air under standard conditions.

To ensure interaction of various types of UAVs as swarm elements, the following requirements must be met:

- Ability to work in the same frequency ranges.
- Ability to use the same signal bandwidth.
- Ability to use the same encoding.
- Compliance with the requirements described above for wireless signal transmitters and receivers and hardware that will implement the formation of data packets according to the proposed algorithms.

If these requirements are met, it will be possible to use various types of UAVs as elements of a same heterogeneous swarm.

4. Formulation of the data transmission with reduced signal power problem for reducing the radio visibility of a UAVs' swarm

Optimizing UAV routes during the mission is the other way of reducing the probability of their loss – the less time the UAV spends in a dangerous area, the better chances it has to avoid air defense and EW means – and the more likely the mission will be completed successfully and/or the UAV will return to the controlled area intact [15]. In addition, due to the limited resource of UAV movement (maximum flight range), the mission simply cannot be completed in certain conditions without optimizing routes.

Also, it is possible to use a steganographic approach to the data transmission from/to UAVs – which means hiding the very fact of transmitting some data [16, 17]. For this, in particular, noise-like broadband signals can be used, but not only them. The UAVs contrast, size and shape must be considered. For example, contrast *C* is defined as the ratio of the difference in luminance between an object and its background to the luminance of its background:

$$C = (B - B_1) / B^1 = \Delta B / B^1, \qquad (6)$$

where *B* is the luminance of the object and B_1 is the luminance of the background in units of cd/m2 [5].

Among the known factors that can affect the wireless network radio visibility reduction, we should highlight the Doppler frequency shift, the height of obstacles to signal propagation (vegetation, buildings, mountains etc.), and the curvature of the earth's surface [18]. But their practical application is significantly limited, because usually the operator cannot choose the terrain on which the mission is to be performed.

One of the ways to increase the UAV movement resource is to save battery charge. This can be achieved, in particular, by reducing the power of transmitted signals (for example, using other UAVs as relay nodes). But at the same time, high-reliability communication should be ensured. This is especially relevant in the case of UAV groups decentralized swarm application, because this mode requires regular interaction between swarm elements [19, 20].

The most common methods of UAV formation management are: "leader–follower", virtual leaders, path following vector fields, fully decentralized approaches based on consensus, approaches based on fuzzy logic [21, 22].

But most known methods of radio transmitter power control are neither automated nor adaptive [23, 24]. Often, they involve manual adjustments to the mutual location of receivers and transmitters and, accordingly, are not applicable to UAV swarms, where the situation and relative location of network nodes can change rapidly and unpredictably.

Thus, it is recommended to develop and use original algorithms for reducing special networks radio visibility, which will consider the above-mentioned specifics.

Formulation of the problem. This section describes the development of such algorithms which, while minimizing the total power level of UAV swarm elements transmitters, would ensure a reliable level of communication between any of the swarm elements.

The first option considered is the use of a mesh network, which would provide direct communication of any swarm element with all other swarm elements at the minimum power required for this, with or without remote control of power from the control center. This option is considered inapplicable for military applications because we will have centralized control of the network. Also, direct connection to all other network nodes is not a necessary requirement for our task.

Encryption must be always used to ensure data security of the dataset *X* during transmission and to maximize their entropy (measure for randomness)

$$H(X) := -\sum_x P(X = x) log_2 P(X = x), \quad (7)$$

where $P(X = x)$ is the probability that the variable X takes on the value x. The bigger entropy is, the harder it is for cryptanalytics to break the cryptographic key and to decipher the data [10].

No data (including service packets) shall be transmitted over the air in an open, unencrypted form.

In addition, the power of signal transmission for each element of the swarm must change dynamically when their mutual location changes, adapting to their movement. So, the swarm elements must independently determine the distance to each other (or the signal quality level). And line-of-sight should be uninterrupted:

$$LOS\ Range = \sqrt{(2 \times (EER) \times H_1) + H_1^2} + \sqrt{2 \times (EER) \times H_2) + H_2^2} \quad (8)$$

where H_1 and H_2 represent the heights of the sender and receiver radio antennas respectively.

Thus, the task is characterized by the following parameters:

Incoming data:

- number of UAVs – swarm elements
- minimum possible signal power

Parameters:

- maximum permissible signal power

Output data:

- routing table of each node with signal strength for each direction

Criterion:

- minimization of the total power of all network nodes while ensuring reliable communication

The result of consideration of the above problem formulation was the approach "Your connection is your business", according to which each UAV builds its own routing table and manages its own power, being responsible for establishing a connection with at least some other network node. The operation of the algorithms developed to implement this approach as an improvement of the algorithms presented in [8, 9, 15, 25] is described below.

5. Development of the improved UAV swarm network initialization algorithm for data transmission and radio visibility reduction

Let's consider the developed data transmission algorithms for protection against radio-electronic warfare and reducing the radio visibility of a UAVs swarm.

Algorithm I. Initialization stage. At this stage, the initial construction of the routing table and the setting of the optimal power of the transmitters for each of the UAVs U_i, i=1…N take place. Procedure:

Phase 1 of initialization. Incomplete routing table.

1. Before starting the task, each UAV U_i among group U that will perform the assigned task and participate in the mission receives a list of these UAVs. So, at the beginning of the mission, each UAV i knows how many UAVs N will participate in the mission, and what their identifiers are.
2. The minimum possible transmitter power of each UAV i is set.
3. Each UAV i sends a broadcast service request RA_i, to which all UAVs in its group, that received this request, must respond. As a result:
4. If no UAV from its group N responded to the RA_i request, the power is increased, and the step 3 is repeated once more.
5. If at least one UAV responded to the request, its identifier is noted in the routing table as directly reachable, and the signal strength required to communicate with it is – also saved.

This completes initialization phase 1. The example at the Figure 1 shows an example of table construction during phase 1.

UAV 1 at the first set minimum power value and was unable to establish contact with any of the other swarm elements. According to step 4, it increased the power level and successfully established communication with UAVs 5 and 7.

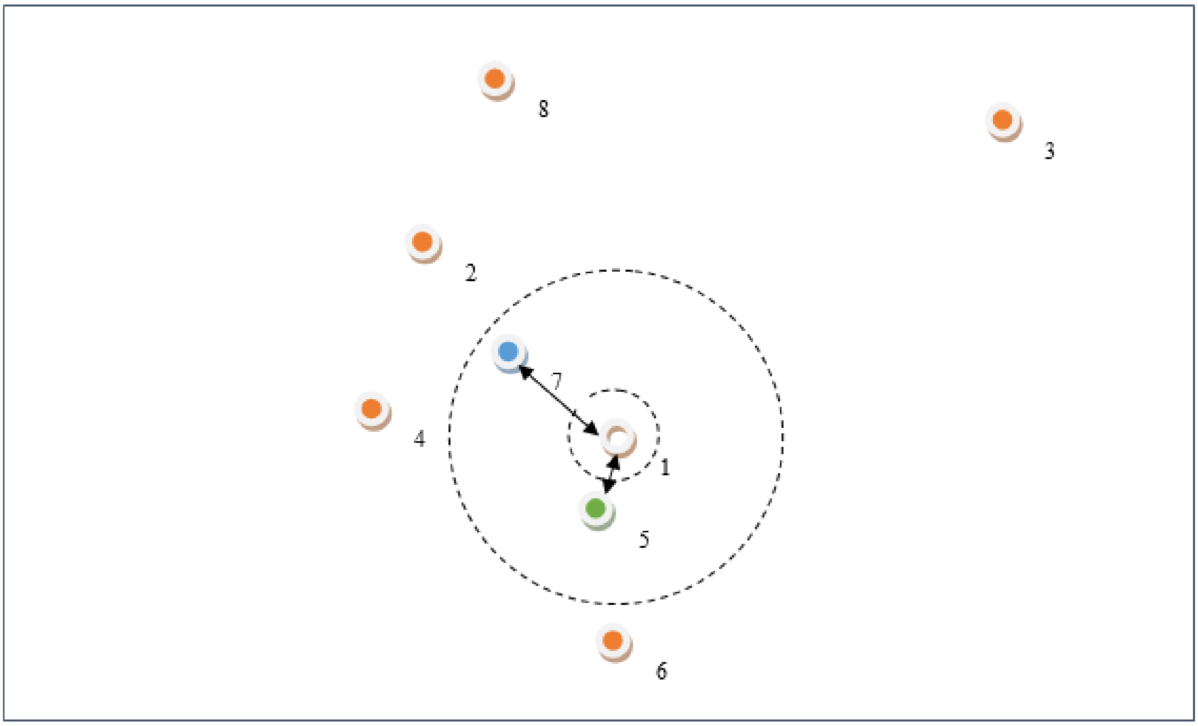

Figure 1: Phase 1 of initialization

Phase 2 of initialization. Routing tables exchange.

6. If during phase 1 of initialization, UAV *i* has received responses from all other UAVs of group *U*, and has fully filled routing table, then phases 2 and 3 of initialization are skipped.

7. Each UAV *i* that does not have a fully populated routing table sends an RB_i request to all UAVs marked in its routing table as directly reachable This is a request to obtain their routing tables.

8. Each UAV *j* that received this RB_i request sends back its routing table TM_j. All, excluding only the line for the UAV *i* itself.

9. After receiving the response from UAV *j*, UAV *i* compares its available UAVs for communication with its routing table. If UAV *k* is absent in its table, but present in the received table, then UAV *i* maintains that UAV *k* is not directly reachable, and communication with UAV *k* must be established through UAV *j*. Also stored is the power level used by UAV *j* to communicate with UAV *k* and whether it is directly or indirectly reachable. Otherwise, this route is saved as an alternative.

10. If multiple UAVs have replied to UAV *i* that they can communicate with UAV *k*, then UAV *i* stores all their IDs and power values in its routing table.

11. Also, through the relay UAVs UAV *i* receives the routing tables of those UAVs that are indirectly reachable – and, if necessary, repeats step 8 for them.

Figure 2 illustrates the second phase of initialization. During the first phase, UAV 1 established communication with UAVs 5 and 7. In the second phase, it exchanges routing tables with them. As a result, it can communicate via relays with UAVs 2, 4, and 6. An example of a routing table after step 2 is shown in Table 1.

As you can see, for some UAVs, we now have more than one route option leading to it.

Phase 3 of initialization. Complete routing table.

1. If UAV *i* has built a fully populated routing table during initialization phase 2, then initialization phase 3 is skipped.

2. If, during phase 2 of initialization, UAV *i* received responses from all directly reachable UAVs of group *U*, but some UAVs remained unreachable (both directly and through relay), this means that a subgroup of UAVs F_t, t=1... M was formed ($M \le N$-1). That is, the members of this subgroup have established communication with each other, but at their current power levels cannot communicate with any other member of group *U*. Then UAV *i* starts successively increasing the power, step by step and sending address requests similar to those in step 3. The only difference is that they are not broadcast,

but intended only for UAVs that are not in his routing table. Other UAVs of this subgroup will do the same.

3. If at some power value UAV *i* received a response from UAV *f* that is not in its routing table, it stores it in the table as directly reachable along with the current power value.

4. Next, UAV *i* broadcasts to all other directly reachable UAVs in its routing table that have established contact with UAV f to add this information to their routing tables.

5. UAV *i* then exchanges its routing tables with UAV *f*, adding to its table the nodes with which the other had direct or indirect communication. Just as on phase 2 of initialization.

6. If, after each UAV of group *U* has reached the maximum power level and exchanged all received results with other UAVs of group *U*, but still has empty lines in the table (i.e., no direct or indirect UAV of the group has been able to communicate with it/them) then this/these UAV is/are considered lost and communication attempts with it/them are stopped.

Figure 3 illustrates the situation after the completion of the initialization phase three.

Table 1
An example of a routing table after phase 2 completion

№	Directly reachable (1 - yes, 0 - no)	Transmission address (for unreachable, otherwise – 0) / power (from a minimum of 1 to a maximum of 10)
2	0	7/3, 4/2
3		
4	0	7/3, 2/2
5	1	0/2, 7/2
6	0	5/2
7	1	0/2, 5/2
8		

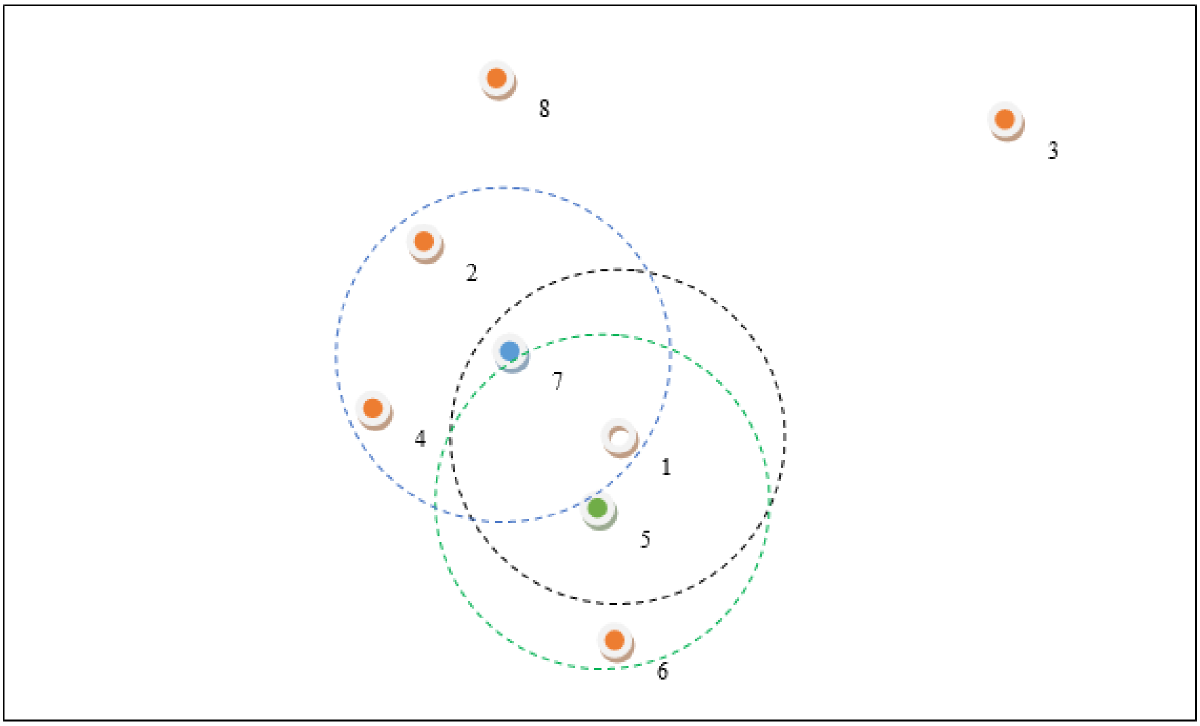

Figure 2: Phase 2 of initialization

Increasing the power step by step, UAV 1 managed to establish communication with UAV 3 (which made a corresponding entry in the routing table presented in Table 2). However, node 8 failed to establish contact with any node due to damage to the transmitter during take-off – therefore it is marked as unreachable.

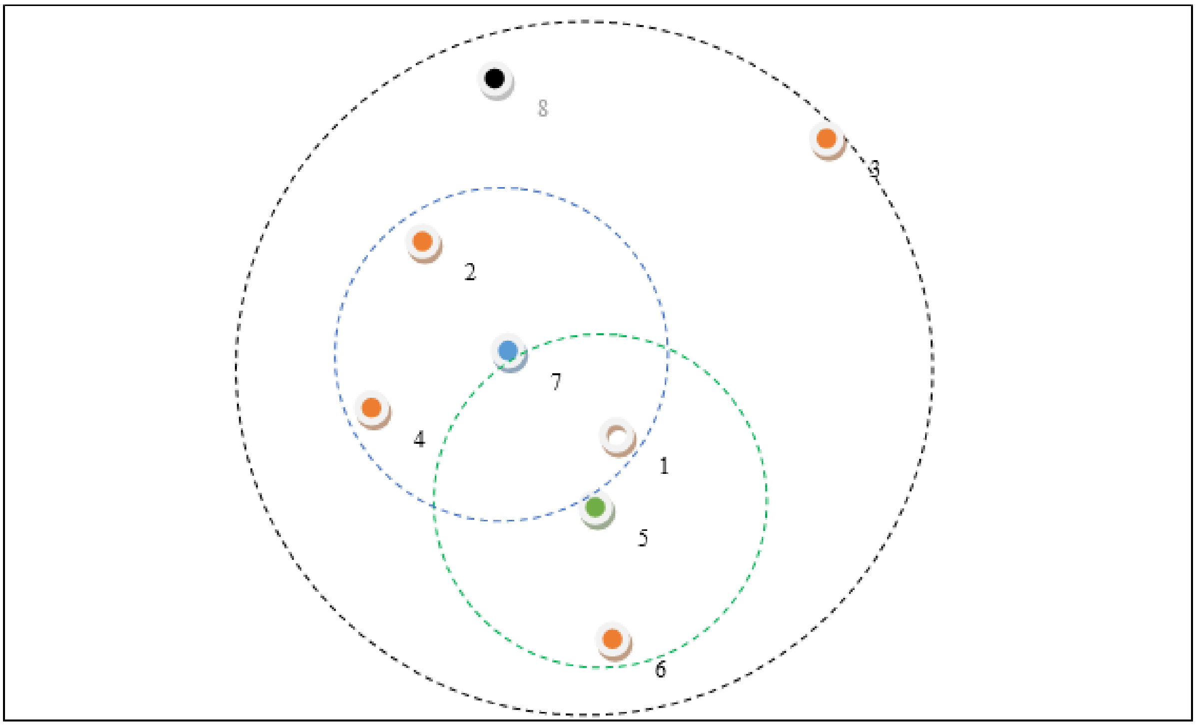

Figure 3: Phase 3 of initialization

Table 2
An example of a routing table after phase 3 completion

№	Directly reachable (1 - yes, 0 - no)	Transmission address (for unreachable, otherwise – 0) / power (from a minimum of 1 to a maximum of 10)
2	0	7/3, 4/2
3	1	0/9, 2/10, 7/10, 5/10
4	0	7/3, 2/2
5	1	0/2, 7/2
6	0	5/2
7	1	0/2, 5/2
8	-	-

This completes the initialization stage. Each UAV *i* has now ready routing table that includes all direct-range UAVs and all options for establishing communication with non-direct-range UAVs (with preserved power level). At the next stage, the optimal route should be selected from the entire set of available routes. Thus, we may solve this problem as the combinatorial optimization problem, which is the main direction of further research for now. After the optimization UAV *i* has a constructed table with optimized routes to all reachable members of group *U*.

6. Development of the improved algorithms that will support further operation of an UAV swarm for data transmission and radio visibility reduction during a mission

Changes in the UAVs relative position are possible while moving along the route while performing the assigned task. The "Pulse" algorithm is used to track them.

"Pulse" algorithm. According to the Pulse algorithm, each UAV pings directly reachable UAVs in its group on a regular basis (during the experiments conducted, once per second value was used). The main principle is that the distance between UAVs does not change dramatically quickly. The algorithm can work in two modes – Reliability and Safety. In Reliability mode, the emphasis is on maximum communication support. If, when communication is lost with a swarm member, increasing the power

by 1 step does not lead to the restoration of communication, the UAV is considered lost. On the other hand, in Safety mode – power increase step is not performed at all, it is assumed that the UAV with which contact is lost will itself try to establish contact with at least some member of the UAV swarm. Algorithm:

1. UAV *i* sending request to all directly reachable UAVs from its routing table at a power level 1 step lower than stored in the routing table. If a response is received from any of these UAVs *k*, UAV *i* stores the updated, lower power level in its routing table for UAV *k*.
2. UAV *i* sends a request to all UAVs except direct-range UAVs at a power level 1 step lower than the maximum among those it is currently using for direct communication. If some UAV *k* was previously marked as not directly reachable, but responded to the request - now it is marked as directly reachable, and the previous communication route with it is saved as an alternative.
3. UAV *i* sends a request to all directly reachable UAVs in its routing table that did not respond in step 1 at the power stored in the routing table. If one of these UAVs *j* did not respond, the communication route with it must be rebuilt according to step 4 and forward. Otherwise, next steps are skipped.
4. If the routing table of UAV *i* has alternative route options to communicate with UAV *j*, then UAV *i* sends them a service packet to attempt to establish communication with UAV *j*. After that, the transmission routes can be optimized considering the updated data. Data about the updated route is transmitted to other UAVs in communication with UAV *i*.

If none of the saved routes allows to establish communication with UAV *j*, then the further step depends on the selected algorithm mode.

5. In the Security mode, no further attempts to communicate with the UAV *j* are made. According to the principle "Your connection is your business", it is considered that UAV *j* itself should take care of establishing a direct connection with at least one other node of the UAV swarm. If he does this, UAV *i* will receive a notification about the updated route. If not, UAV *j* will be considered lost.
6. In Reliability mode, UAV *i* increases the transmission power level to communicate with UAV *j* by one step and tries to establish communication again. It is believed that since the “Pulse” algorithm works regularly, UAV *j* could not move away fast enough to lose contact even at the power increased by one step. If, even in this case, no response is received from UAV *j*, further attempts are terminated according to the approach described in point 5.
7. UAV *i* sends a request to all UAVs except direct range UAVs at the maximum power level among those it is currently using to establish direct communication with *j*. If some UAV *k* was previously marked as not directly reachable but responded to the request – now it is marked as directly reachable, and the previous communication route with it is saved as an alternative.

External adjustment. The external adjustment algorithm is applied if a request is received from a UAV currently marked as unreachable or directly unreachable in the routing table.

1. If the UAV swarm element *i* receives a request from UAV *k*, which is marked as not directly reachable or unreachable in the routing table of UAV *i*, corresponding changes are made to the routing table of UAV *i* – UAV *k* is now marked as directly reachable.
2. UAV *i* sends updated information to all UAVs in direct range (except UAV *k*) so that they can adjust their own routing tables to account the position changes.

This is applied when any of the network nodes have joined the network (or come within direct link distance) to account for this change.

7. Analysis of advantages and disadvantages of the improved algorithms compared to its previous version

Algorithms testing for checking their pros and cons was provided in laboratory conditions on the basis of two pairs of Ettus B200 and HackRF One software-controlled programmable radio stations, shown on Figure 4. They are applicable because of their support of the signal power control.

Applied tests has shown that algorithms are practically applicable. Further testing, using bigger amount of programmable radio stations (preferably on the basis of real UAVs), is another direction of further research, but this requires purchasing additional hardware.

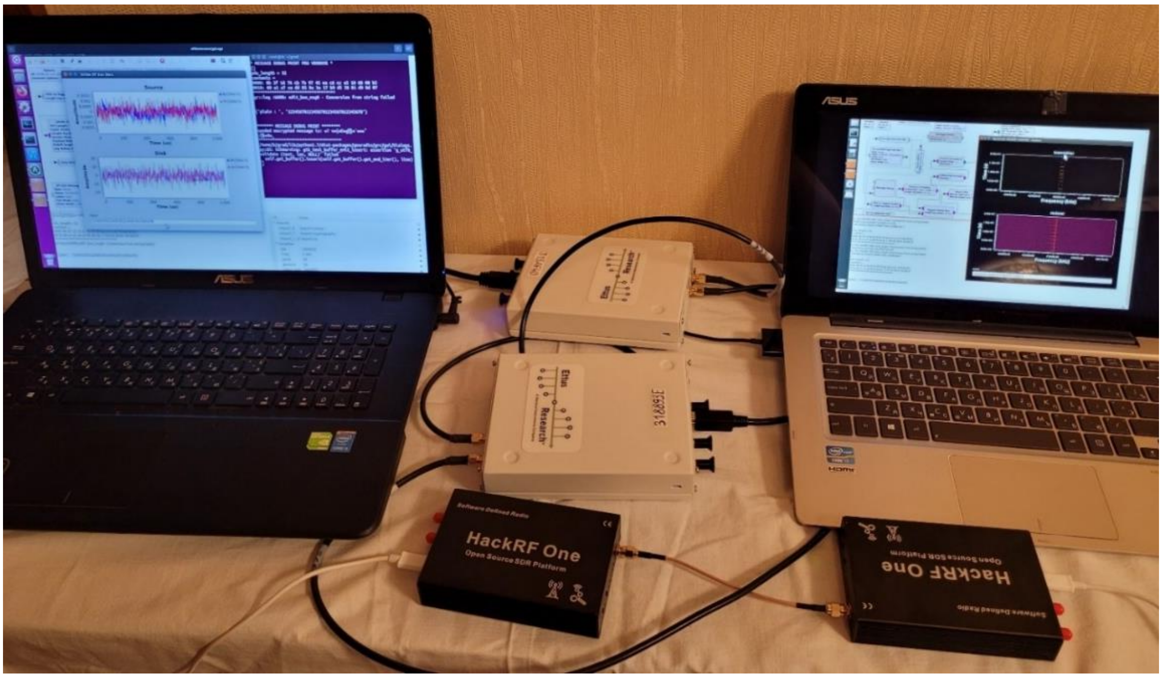

Figure 4: Laboratory stand on the basis of Ettus B200 and HackRF One radio stations

Comparing improved algorithms to their previous versions: main advantage of the improved algorithms compared to the previous version is presence of the phase 2 – routing tables exchange. It saves time during initialization, as reduces the number of requests to build routing tables. Additionally, in many situations it gives alternative routes, which allows to optimize data transmission routes between UAV swarm elements. A number of other changes have also been made that increase the performance and/or reliability of the algorithm, or reduce the radio visibility of the UAVs swarm, in particular, the Reliability and Safety modes have been added.

Let's consider the results of the analysis of the advantages and disadvantages of the developed improved algorithms for reducing the UAV swarm radio visibility. Let's start with the advantages:

- Due to power management and minimization of its overall level, the probability of detection of the UAV swarm by the enemy during the mission is reduced – and therefore, the probability of the destruction for every UAV is reduced. Thanks to this, the probability of successful mission completion increases.
- By minimizing the power of the UAV transmitters, the battery charge is saved – and the flight range of the UAV in swarm increases accordingly.
- The algorithms are resistant to changes in the mutual position and composition of UAVs within the swarm during the execution of the assigned task.

Disadvantages of the developed improved algorithms for reducing the radio visibility of the UAVs swarm:

- It is necessary to form a UAV swarm in advance to perform the assigned task and upload their identifiers to each UAV
- A rather complex scheme of routing tables distribution and update
- Additional exchanges of service data packets for power management slightly (although experiments shown, that not very significantly) reduce the bandwidth of data transmission channels

None of the identified shortcomings leads to a decrease in the value of the obtained results.

8. Conclusions

The result of the work carried out in this publication is an improved family of algorithms for reducing the UAVs transmitters power during data transmission between nodes of a UAV swarm for military applications (although civil application for saving swarm batteries is also possible). Its use will ensure the necessary communication quality, minimizing radio visibility, and therefore, reduces the probability of UAVs detection and destruction, while providing an opportunity to save the battery charge, thereby increasing the UAVs operational time.

The main direction of further research is solving the combinatorial optimization problem of building optimal route for data transmission from the UAV *i* to any other UAV from its swarm, for which it has more than one route in its routing table. Additional directions for further research:

- Further testing of the developed algorithms, using bigger amount of programmable radio stations (preferably on the basis of real UAVs), is another direction of further research, but this requires purchasing additional hardware.
- Determining (with real UAVs) the optimal value of the routing table reconstruction period.
- Determining the level of energy saving when applying the algorithm.

9. References

[1] R. E. Weibel, R. J. Hansman, Safety considerations for operation of unmanned aerial vehicles in the national airspace system, MIT International Center for Air Transportation Department of Aeronautics & Astronautics Massachusetts Institute of Technology Cambridge, USA, 2004. doi:10.2514/6.2004-6421.

[2] Otto, A., N. Agatz, J. Campbell, B. Golden, and E. Pesch. "Optimization approaches for civil applications of unmanned aerial vehicles (UAVs) or aerial drones: A survey." Networks, 72(4) (2018): 411–458.

[3] Xu, C., H. Duan, F. Liu. "Chaotic artificial bee colony approach to uninhabited combat air vehicle (UCAV) path planning" Aerospace Science and Technology 14, 8 (2010): 535-541. doi:10.1016/j.ast.2010.04.008.

[4] S. S. Ponda, L. B. Johnson, A. Geramifard, and J. P. How, Cooperative mission planning for multi-UAV teams, in: Handbook of Unmanned Aerial Vehicles, Dordrecht, Springer, 2015, pp. 1447-1490. doi:10.1007/978-90-481-9707-1_16.

[5] R. Austin, Unmanned Aircraft Systems. UAVs Design, Development And Deployment. – West Sussex: John Wiley and Sons, 2010. – 365 p. doi:10.1002/9780470664797.

[6] K. Yereke, UAV classification and their control method types, Editorial Board, 2022, p.769.

[7] Lagkas, T., V. Argyriou, S. Bibi, and P. Sarigiannidis. "UAV IoT framework views and challenges: Towards protecting drones as "Things"." Sensors, 18(11) (2018): 4015. doi:10.3390/s18114015.

[8] M. I. Ogurtsov, Development of a cryptographic algorithm for the protection of UAV swarms wireless communication channels, in: Proceedings of the XXVI international conference "Actual problems of applied mathematics and computer science APAMCS-2021", Ivan Franko National University of Lviv, Lviv, 2021 pp. 133-136.

[9] Ogurtsov, Maksym. "High-Reliability Data Transfer Algorithm with Reduced Transmitters' Power for Use in Special Networks" International Journal "Information Content and Processing", Volume 6, Number 1, 2019: 79-90. (in Ukrainian).

[10] N. Ferguson, B. Schneier, T. Kohno, Cryptography engineering: design principles and practical applications, John Wiley & Sons, 2011.

[11] Liu, J., N. Sha, W. Yang, J. Tu, and L. Yang. "Hierarchical Q-learning based UAV secure communication against multiple UAV adaptive eavesdroppers". Wireless Communications and Mobile Computing 2020 (2020): 1-15. doi:10.1155/2020/8825120.

[12] Gan, J., A. Hu, Z. Kang, Z. Qu, Z. Yang, R. Yang, and J. Zhou. "SAS-SEINet: A SNR-Aware Adaptive Scalable SEI Neural Network Accelerator Using Algorithm–Hardware Co-Design for High-Accuracy and Power-Efficient UAV Surveillance". Sensors, 22(17), (2022): 6532. doi:10.3390/s22176532.

[13] Z. Ahmed, A. Ahmad, M. Altaf, and F. A. Khan. "Power efficient UAV placement and resource allocation for adaptive video streaming in wireless networks". Ad Hoc Networks, 150 (2023): 103260. doi:10.1016/j.adhoc.2023.103260.

[14] Matsuda, T., M. Kaneko, T. Hiraguri, K. Nishimori, T. Kimura, A. Nakao. "Adaptive direction control for UAV full-duplex relay networks using multiple directional antennas". IEEE Access, 8 (2020): 85083-85093. doi:10.1109/ACCESS.2020.2992293.
[15] M. Ogurtsov, V. Korolyov, O. Khodzinskyi, Improving the Productivity of UAV Operations Based on Granular Computing and Fuzzy Sets, in: 2021 IEEE 6th International Conference on Actual Problems of Unmanned Aerial Vehicles Development (APUAVD) 19-21 Oct. 2021, 2021, pp. 33-36. doi:10.1109/APUAVD53804.2021.9615419.
[16] Cheddad, A., J. Condell, K. Curran, and P. Mc Kevitt. "Digital image steganography: Survey and analysis of current methods". Signal processing, 90(3) (2010): doi:727-752. 10.1016/j.sigpro.2009.08.010.
[17] O. Lavrynenko, A. Taranenko, I. Machalin, Y. Gabrousenko, I. Terentyeva, D. Bakhtiiarov, Protected voice control system of UAV, in: 2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD), IEEE, 2019, pp. 295-298. doi:10.1007/978-3-319-78816-6_9.
[18] Maladyka, Ihor, Stas Serhiy, Mykhailo Pustovit, and Oleksandr Dzhulay. "Application of UAV Video Communication Systems During Investigation of Emergency Situations". Advances in Science and Technology 114 (2022): 27-39. doi:10.4028/p-7tt2j8.
[19] H. Hamann, Swarm robotics: a formal approach, Springer International Publishing, 2018. 210 p. doi:10.1007/978-3-319-74528-2.
[20] N. Correll, M. Schwager, M. Otte, Distributed Autonomous Robotic Systems: The 14th International Symposium, Springer Nature Switzerland AG, 2019. 528 p. doi:10.1007/978-3-030-05816-6.
[21] Zhou, Yongkun, Bin Rao, and Wei Wang. "UAV swarm intelligence: Recent advances and future trends." Ieee Access 8 (2020): 183856-183878. doi:10.1109/ACCESS.2020.3028865.
[22] Campion, Mitch, Prakash Ranganathan, and Saleh Faruque. "A review and future directions of UAV swarm communication architectures." 2018 IEEE international conference on electro/information technology (EIT). IEEE (2018). doi:10.1109/EIT.2018.8500274.
[23] Sahu, Biranchinath, and Gabriel A. Rincón-Mora. "Adaptive Power Management of Linear RF Power Amplifiers in Mobile Handsets—An Integrated System Design Approach." Submission for IEEE Asia Pacific Microwave Conference. (2004). doi:10.1109/MWSYM.2001.967189.
[24] Chen, Xi, Ming Ma, and Anfeng Liu. "Dynamic power management and adaptive packet size selection for IoT in e-Healthcare." Computers & Electrical Engineering 65 (2018): 357-375. doi:10.1016/j.compeleceng.2017.06.010.
[25] Maksym Ogurtsov. "Review of Neural Networks Application in UAV Routing Problems." International Scientific Symposium «Intelligent Solutions» IntSol-2021, September 28–30 2021, Kyiv-Uzhhorod (2021): 45-54.