System for Simultaneous Control of Multiple Unmanned Aerial Vehicles

Yehor Zheliazkov
SBH Nordost GmbH, Dresden Chip Academy, Hermann-Reichelt Str. 3A, 01109 Dresden, Germany
yzheliakov2@gmail.com

Keywords: Unmanned Aerial Vehicles, Swarm Drone, Software-Defined Radio, Over-The-Air.

Abstract: Nowadays, airspace is a strategically important resource for both national security and economic development. The state is responsible for its efficient use and safety. One of the key challenges of today is countering unmanned aerial vehicles, which includes the use of electronic warfare, laser weapons and other technologies. The popularity of drones is growing rapidly not only in the consumer sector, but also in industry, agriculture, energy, geodesy, and military. Military conflicts demonstrate a significant increase in the use of unmanned aerial vehicles, in particular in the form of drone swarms, which creates new challenges for countermeasures. One of the most promising developments is the creation of a platform for managing heterogeneous swarms of drones, including those that were previously hostile but can be integrated into their own system. It provides new opportunities for warfare and an advantage in the management of military operations. This paper presents solutions that provide simultaneous control over heterogeneous unmanned aerial vehicles, which makes it difficult to use them effectively in modern warfare and defense strategies. An approach is realized as real prototype electronics circuit, which can create a flexible platform capable of intercepting, analyzing and integrating enemy unmanned aerial vehicles into its own network through electronic interference, hacking communication protocols and reprogramming. The results of proposed approach case study showed the possibility to take under the control “enemie’s” unmanned aerial vehicles to the control of main operator.

1 INTRODUCTION

Globally, airspace is an important resource for various sectors of national security and the economic sector. It is the duty of the state to ensure the efficient use of airspace and its security [1].

Today, new ways of countering unmanned aerial vehicles (UAVs) are being explored, including the use of electronic suppression means - various electronic warfare (EW) devices, as well as directed energy emission means - laser weapons [1, 2].

Until recently, there has been a rapid increase in the popularity of drones, and it was based on everyone's interest in flying. Photo and video recording from the air, the ability to shoot in previously inaccessible places, new angles - all this made the technology in demand. Drones topped the charts of the most desired gifts in the consumer market. But UAVs are not just a hobby or a selfie, they are becoming assistants in various industries: agriculture, mining, topography, geodesy, and energy. All of these are industrial and economic sectors [1].

Dominance in space gives an advantage over the enemy in controlling troops and weapons. This is facilitated by electronic warfare (EW) and electronic warfare (EW) means, which are one of the leading elements of current wars and armed conflicts and have the highest development dynamics among all modern weapons [3].

The experience of current military conflicts and the war in Ukraine shows the growing role of drones and the variety of their models (air, surface, ground) on the battlefield for various functional purposes. At the same time, there is an active use of not only single UAVs, but also a large number of them simultaneously. The nearest modern prospect is the transition to swarms of drones [4].

Military and civilian life are undergoing a profound transformation based on advances in two critical technologies: machine autonomy and artificial intelligence (AI). The current global trend is the creation and use of various sets of drones - drone

swarms - which is already revolutionizing the way we look at military art [4].

At the moment there is no platform that can simultaneously control a swarm of unmanned aerial vehicles (UAVs) of different models and different purposes, including those that belonged to “enemies” and are becoming “our own”.

The main aim is to develop a new drone control platform capable of controlling a swarm of unmanned aerial vehicles with the ability to simultaneously control different models of drones, as well as the ability to “intercept” enemy UAVs at close range.

2 THE PRINCIPLE OF CONTROLLING A SWARM OF UNMANNED AERIAL VEHICLES

2.1 The Principle of Controlling a Swarm of Unmanned Aerial Vehicles

In a group of drones interacting based on swarm intelligence, each of the devices interacts only with some of the devices closest to it now [5]. At the same time, energy consumption for information transmission is relatively low. UAVs make decisions about their current behavior based on self-collected environmental data as well as data transmitted by neighboring vehicles. Energy-consuming communication with the central control device is carried out only to receive information about the tasks assigned to the group and to transmit a report with information about the group's status during the implementation of the completed tasks [5]. The swarm algorithm is an effective solution to ensure optimal control of a UAV swarm [6].

According to [5], a simplified general scheme of swarm intelligence algorithms includes the main stages:

1) Initialization of the population - this stage initializes (often randomly) the population of agents that are given directions to search for targets;
2) Migration of agents (finding targets, exchange of information between agents, changing the target if other agents have found a higher priority target);
3) Completion of the search (occurs if all the found targets have been achieved).

The swarm algorithm in the form of a flowchart is shown in Figure 1.

This algorithm is the basis for the further creation of any other UAV swarms related to management and communication in the group. The authors in [5] also provide bee swarm algorithms for controlling a UAV swarm and responding to emergencies separately, which is also an additional basis for building a UAV control interception algorithm.

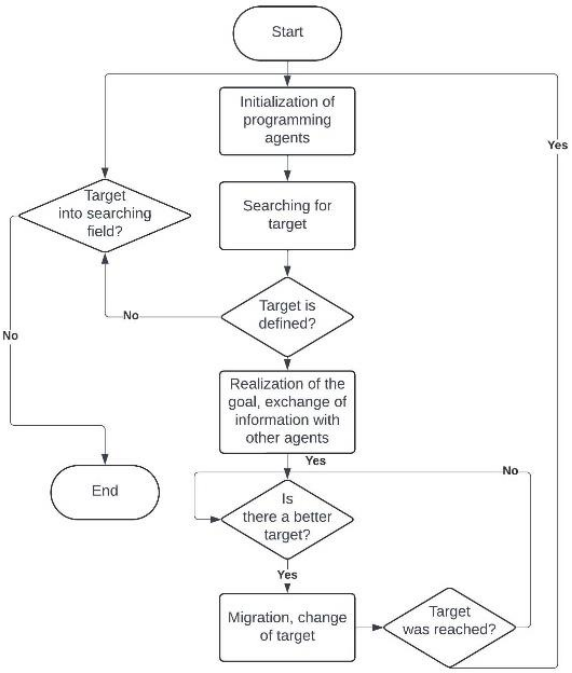

Figure 1: The general swarm algorithm.

In order to implement the algorithm, you need to know all the components for its construction. The main aspects:

1) The ability to remotely flash the device.
2) Compliance of the UAV module for remote flashing.
3) The ability to identify the drone within range

2.2 Wiring Diagram of the Device for Intercepting and Repurposing an Enemy Drone

The description of the connection scheme of a device for intercepting and repurposing an enemy drone consists of three important components: a signal interception circuit, a reflashing circuit, and a signal jamming circuit.

General flowchart for intercepting and repurposing an enemy drone is shown in Figure 2. It was suggested similar as in [7].

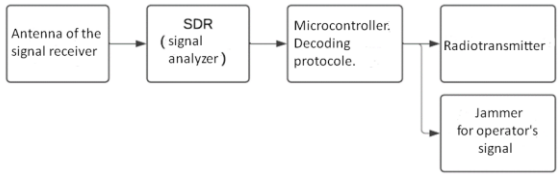

Figure 2: Flowchart for intercepting and repurposing an enemy drone.

The following steps should be taken into account in order to realize this:

1) To receive a signal, connect the antenna to a radio receiver for analyzing Software-Defined Radio (SDR) signals, in particular, to analyze the frequencies at which the drone operates. SDR is designed to analyze the frequency spectrum and data transfer protocols between the drone and its operator.
2) Protocol decoding. It is necessary and sufficient to study the structure of protocol packets (MAVLink, DSMX or other protocol).
3) Generation of a replacement signal. An RF transmitter connected to the microcontroller is used to generate commands.
4) Blocking the operator signal. The jammer generates intense noise on the control channel.

Instead of the conventional “jammer”, another gun is implemented, which sends a pulse that the drone “understands”. The software is flashed with the help of “Over-The-Air” (OTA); in particular, “migration programming” is used [8]. The “gun” itself must have the appropriate software for reprogramming.

There must be a corresponding module for each remote flashing. One of the components of any UAV is a flight controller, or control module. A flight controller is a UAV control board that processes signals from its own sensors (accelerometer, gyroscope, etc.), devices connected to it, pilot commands, and calculates the speed to be set for the motors [9].

The controller has possible corresponding interfaces (UART, I2C, PWM, etc.) for connecting ESC, VTX, RX, camera, GPS, servomotors, and other devices. The mentioned interfaces for remote flashing must be compatible with OTA updates [9].

2.3 Scheme for Signal Interception

To implement the hardware to intercept and repurpose an enemy drone, you need a circuit that includes elements for analysis, jamming, device connectivity, and reflashing. Below are the main components and their roles in the circuitry implementation.

The main components of the hardware circuit include: a radio receiver for signal analysis - Software-Defined Radio (SDR); a transmitter for signal replacement, a signal jammer, an interface for connecting to the drone, microcontrollers, sensors for debugging and testing signals [10].

Components:

1) Receiving antenna (e.g., Yagi type directional antenna);
2) SDR module (HackRF, RTL-SDR) for analyzing control signals;
3) Microcontroller (STM32/Arduino) for signal processing;
4) Radio transmitter (nRF24L01, CC2500) for transmitting new commands to the drone.

The antenna is connected to the SDR via an SMA connector. The SDR is connected to a computer (PC) via USB. The PC is used to analyze the frequency and signal protocols using software (e.g. GQRX, SDR#). After analyzing the signal, the PC transmits the protocol information to the microcontroller via UART or USB.

The microcontroller generates data packets and transmits them to the RF transceiver via SPI.

3 STRUCTURE SCHEME

To take control of the drone, the system first intercepts the signal, then analyzes the protocol, and then transmits commands, labeling the operator's signals, via the RF module.

A “cannon” circuit for implementing the principle of intercepting a third-party UAV is proposed, as shown in Figure 3. The power supply provides stable DC and AC voltages for all system components - 3.3 V, 5 V, and 230 V. The microcontroller (MCU) is the main component of the system, responsible for signal processing, coordination of other modules, and execution of the interception algorithm. The MCU exchanges signals via digital pins to communicate with the radio frequency module (RF module) and the signal jammer.

In this paper, we consider a new device with the ability to intercept and control a swarm of UAVs using jamming and spoofing capabilities.

A signal jammer is a device that interferes with a drone's signal, causing the UAV to either lose its signal and fall from the sky or return to the operator.

By hacking the UAV system, it becomes possible to take control and fly in any direction.

Based on the received signals, the microcontroller performs calculations to determine the type of

protocol and drone control parameters, and connects to the drone to gain control.

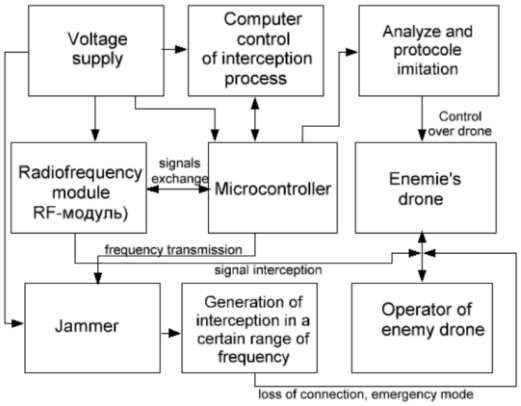

Figure 3: Block diagram of the system for intercepting an unauthorized UAV.

The RF module is responsible for intercepting signals [11] used in communication between the enemy drone and its operator. Sequence of the module operation:

- The microcontroller initializes the module via the SPI interface; the microcontroller transmits frequency data to the signal jammer;
- the jammer generates interference in a certain frequency range;
- The UAV loses communication with the operator and goes into emergency mode.

3.1 Stage of Signal Jamming

The jamming stage is the key to blocking communication between the enemy drone and its operator. Here is a sequential description of the process:

1) Determining the control frequency:
   - Before jamming, it is important to determine the operating frequency that the drone uses for communication. Common frequencies used for FPV are 900 MHz, 1.2 GHz, 1.3 GHz, 2.4 GHz, 3.3 GHz, and 5.8 GHz. The device must be capable of working with the appropriate frequencies [12].
   - Signal intensity (RSSI) is used to determine the exact channel on which communication is taking place [13]. Since the signal strength changes throughout the flight, communication degradation can be assessed in advance, more smoothly and before "problems" in control occur - this is an advantage of RSSI. The signal strength can be determined on both analog and digital receivers.
2) Setting up the jammer. To jam the signal, you need to set the exact frequency of the channel where the UAV operates. Then adjust the interference width to cover the drone's signal [14].
3) Generating interference. The jammer transmits a powerful signal of the same frequency as the operator's signal, but with high intensity (usually > 10 dB stronger). This creates "noise" that prevents the drone from receiving commands. The jamming method used is broadband jamming, which creates noise in the entire frequency range [15].

3.2 Signal Interception Stage

The signal interception phase involves several steps, each of which is critical to successfully seizing control of the drone.

Sequential description of the process:

A) Setting up the RF module to listen for frequencies. The RF module is configured on the microcontroller via the SPI interface [16]. The main parameters are: a) frequency range (in most drones it is 2.4 GHz), the RF module starts scanning channels in the range; b) data rate (common rates are 250 kbps, 1 Mbps, 2 Mbps); c) channel width (1, 2 or 5 MHz).

B) Scanning the frequency range. The RF module switches to the "receive" mode (RX-mode) to listen for signals within 2.4 GHz. The module checks each channel and records the activity of the signals (for example, RSSI level - radio signal intensity) [17].

C) Intercepting a data packet. Once a signal is found, the RF module stores the data packet in its buffer, and the microcontroller reads the packet via the SPI interface for further analysis. The packet includes the drone's ID, transmitter address, and commands (e.g., "takeoff", "turn"). If activity is detected on a particular channel, the microcontroller stops scanning and starts analyzing the signal.

D) Determination of communication parameters. The microcontroller analyzes the received packet and extracts important parameters: 1) the transmitter address - a unique ID of the operator to which the drone is connected; 2) control commands that are decoded depending on the protocol; 3) cyclically redundant CRC code - checking the correctness of data to avoid errors [18]. The

collected parameters are stored in the microcontroller's memory: 1) signal frequency; 2) drone address; 3) communication protocol.

The microcontroller uses these parameters to connect to the drone and send its commands.

3.3 The Stage of Transferring Control to the Enemy UAV

The main requirements for successful UAV interception are accurate collection of drone communication parameters (ID, frequency, packet structure), quick setup of the RF module (interception and connection takes fractions of a second), and stable operation of the jammer (to maintain control advantage) [19].

The process of transferring control to an enemy UAV involves several stages that are performed sequentially:

1) Interception of the signal from the drone. The RF module operates in a given frequency range, it is configured to listen to signals coming to the UAV from its operator. When the microcontroller receives these signals through the RF module, it:
   - Analyzes the signal structure (communication protocol, data rate, transmitter address).
   - Records the parameters used for communication (drone ID, command codes).
2) Protocol analysis and simulation. After intercepting the signal, the microcontroller performs analysis [20]:
   - Determines the type of communication protocol (e.g., DSMX, SBUS, or other).
   - Decodes the structure of the data packet (commands transmitted by the drone operator, for example: movement, ascent, landing).
   - Generates new data packets that simulate the operator's signal.
3) The RF module is set to the same communication parameters as those used by the drone operator. These parameters include signal transmission frequency, recipient address (drone ID), and data rate (bits/s).
4) Blocking the real operator's signal. To prevent the UAV from receiving signals from its original operator, the jammer generates radio interference on the frequency used by the operator [21]. This blocks signals from the control panel to the drone, leaving your device as the only source of commands. The microcontroller fully controls the UAV through the RF module, including transmitting commands (e.g., “Raise the UAV to a certain height,” “Land at a given point,” “Turn off the engines”). The commands are formed in accordance with the structure of the protocol that the UAV is waiting for.
5) Support for stable control. The microcontroller constantly communicates with the UAV, periodically sending confirmation or new commands. The signal jammer continues to block the signals of the real operator.

4 CALCULATING THE RANGE OF ACTION

During the operation of the radio module, there is a permanent exchange of messages between the receiver and the transmitter. Under normal operating conditions, the receiver responds to the transmitter with a response about the correct reception of the information packet. Thus, the calculation of the potential range can be reduced to the calculation of the range of the radio line with an active response. Figure 4 and Figure 5 show the structural diagrams of the radio-controlled system (RCS) and the control panel in a simplified form. According to fig. 4, the radio-controlled system has an antenna, a module for radio control, which can be performed by the certain chip [16].

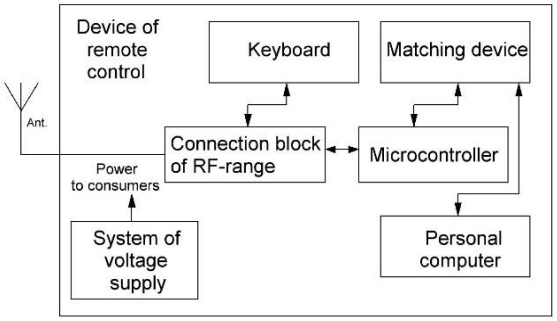

Figure 4: Radiocontrol system for signal receiver.

Diagram of the remote control. Ours is a remote control, which is implemented on the basis of the NRF24L01 chip. In addition to the chip itself, the remote control may contain additional amplifiers and an antenna that also provides amplification.

In this case, it is important to connect with main drone among the swarm of unmanned aerial vehicles. It is difficult technology with different parameters and internal algorithms for drone detection, especially when they different distance and different construction have, which may difficult to determine.

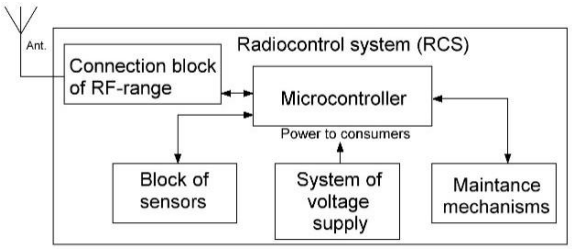

Figure 5: Signal transmitter as device of remote control.

In the most of situation people use the chip NRF24L01. In addition to the chip itself, the RCS communication unit may contain additional amplifiers and an antenna that also provides amplification [16].

To calculate the potential range of the RFS use the theory of the potential range of an active response radio line. The maximal possible range in free space, in the absence of active and passive interference, do not taking into account attenuation in the atmosphere, is determined by the equation:

$$R_{\max} = \sqrt{\frac{P_{Tx} G_{pkc} G_{n\delta y} G_{nrf} \lambda^2}{(4\pi)^2 P_{\min}}} \qquad (1)$$

P_{Tx} is maximum transmitter power of the radio module (W), $G_{n\delta y}$ is the gain of the remote control antenna, G_{pkc} is the antenna gain of the RCS, P_{min} receiver sensitivity (W), R_{max} is maximal possible range (m), G_{nrf} is additional gain (taking into account possible additional amplifying).

Taking into account the fact that the calculations are made for a ground-moving platform, it is necessary to pay attention on the line-of-sight range, since this frequency range does not provide for operation without line-of-sight [17-18]. There was used the line-of-sight range equation:

$$D_{\max} = 4.12\left(\sqrt{H_a} + \sqrt{h_b}\right) \qquad (2)$$

H_a is height of the remote control antenna, h_b is height of the RCS antenna.

A comparison of the possible range of the radio control system (R_{max}) with the distance to the radio horizon (D_{max}), which is determined by the design of the control station's antenna mounting and elevation system, shows a way to increase the range of the control system [19-20].

There are two ways to increase the efficiency of the system: to introduce additional signal amplifiers into the system, or to build an antenna system with a higher gain.

Taking into account for NRF24L01 technical characteristic (frequency – *2.4 GHz*, control station antenna height – *1.5 m*; control station antenna gain *20 dB*; the height of the antenna on the mobile platform is *0.1 m*; the pin antenna gain on the mobile platform – *5 dB*) and parameters defined by programmatic agencies (NRf24 receiver sensitivity – *-85 dBm*; data transfer rate – *1 Mbps*; transmitter output power – *0 dBm*), were received from (1) and (2) distance parameters such as R_{max}≈*3.12 km* and D_{max}≈*6.35 km* [21].

5 PRACTICAL REALIZATION OF DEVICE

Distance parameters such as *Rmax≈3.12 km* and *Dmax≈6.35 km*. It is enough to maintain of Swarm Drone, because the plural average of drones are flying near each other with a distance less than 100 m. As the result, it was built the circuit in Figure. 6.

Device in Figure 6 takes into account two PLL-synthesizers ADF4351. The ADF4351 synthesizer is used as the basis and signal source for jamming. The output signal of the RF interference is formed by mixing the signal of the local oscillator and the signal of the intermediate frequency noise. The intermediate frequency signal is generated by amplifying and filtering the base noise. The local oscillator signal is generated from the ADF4351 signal generator. Since the frequency of the local oscillator can be changed using the ADF4351, the center frequency of the RF signal can be controlled by program [22].

The second ADF4351 has a built-in voltage controlled oscillator (VCO) with a fundamental output frequency in the range of 2200 MHz to 4400 MHz. In addition, the 1/-2/-4/-8/-16/-32/-64 divide-and-convert circuits allow the user to generate RF output frequencies up to 35 MHz. All on-chip registers are controlled via a simple 3-wire interface [22]. The device operates from a power supply in the range of 3.0 V to 3.6 V and can be turned off when not in use.

It takes into account: PLL-synthesizer (ADF4351), flashing device (ST-Link V2), microcontroller (STM32), RF-Transceiver intercepting (NRF24L01) and another additional components. Detailed scheme of device is represented in Figure 6.

Radio frequency (RF) enables communication between a drone and its ground transmitter or remote control, typically operating in the 2.4 GHz to 5.8 GHz range – with 2.4 GHz and 5.8 GHz being the most commonly used frequencies for remote drone control.

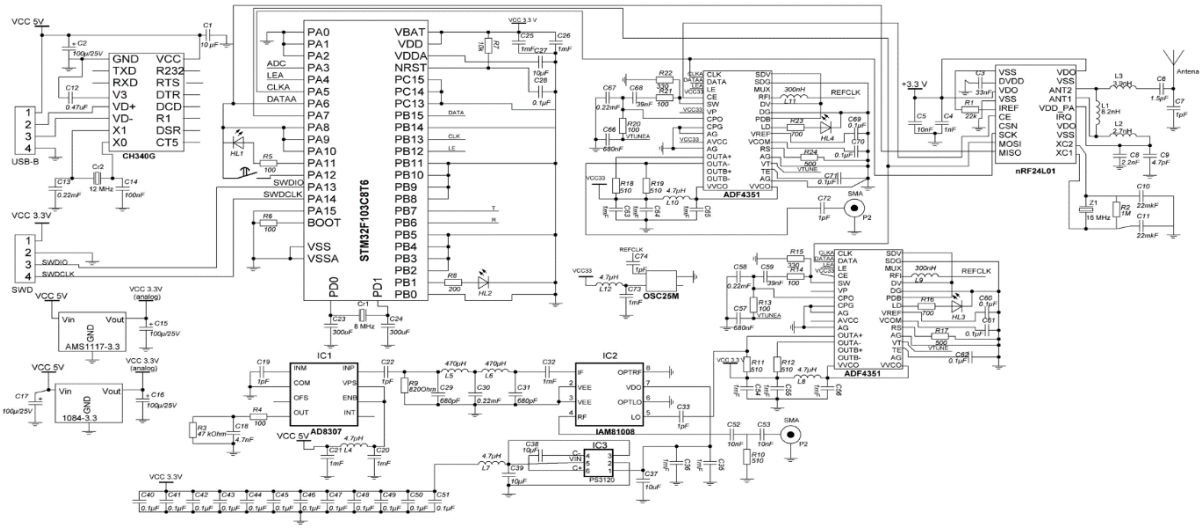

Figure 6: Electronic circuit diagram for UAVs intercepting.

Designing a loop filter is a key part of PLL design. In order to obtain a stable VCO control voltage, a loop filter should be used to filter out high-frequency interference in the line voltage [23]. In this work, a passive low-pass notch filter of two orders is used. System for simultaneous control of multiple unmanned aerial vehicles means that there is main drone among the swarm of drones and one drone can arrange synchronized work for other nearest UAVs. After the jamming antenna receive the signal with a following processing and then sends the feedback signal with remotely update firmware using official applications and OTA technologies. Code takes into account programming for ADF4351 and STM32, which are connected to each other:

```
   for (uint32_t freq = 100000000; freq
<= 1000000000; freq += 1000000) {
   ADF4351_set_frequency(freq);//freque
ncy
   HAL_Delay(10); // wait for Stabil PLL
   uint16_tadc_value                  =
HAL_ADC_GetValue(&hadc1);
   float              voltage          =
convert_adc_to_voltage(adc_value);}
```

In an RF jamming attack, the attacker first identifies the drone's active communication channel and then tunes into that frequency. RF jammers emit stronger signals on the same frequency as the target, overwhelming the receiver and preventing it from decoding legitimate signals [24]. Figure 7 illustrates a RF jamming attack scenario. Swarm drones are working through the protocols [9] and this system hacks not only main drone, but also auxiliary drones among the swarm.

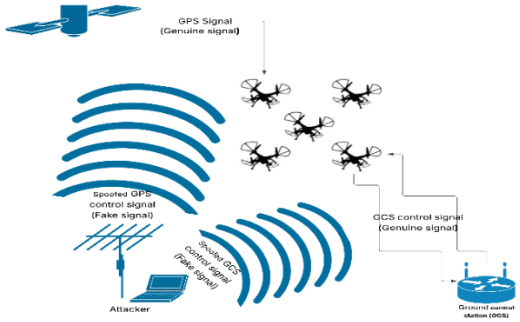

Figure 7: Schematic realization of jamming and spoofing attacks.

CONCLUSIONS

A new drone control platform has been developed which differs from famous by capability of controlling a swarm of unmanned aerial vehicles with the ability to simultaneously control different models of drones. During the research it was hacked 5 swarm drones, which take into account 1 main and 4 auxiliary.

The description of the wiring diagram of a device for intercepting and repurposing an enemy drone consists of three important components: a signal interception circuit, a reflashing circuit, and a signal jamming circuit. It is enough to use possible range in free space of 3.12 km and range of 6.35 km for hacking the swarm of drones.

For most modern drones from well-known manufacturers (e.g. DJI), it is possible to remotely update the firmware using official applications and

OTA technologies. However, the drone must be connected to the Internet via a controller or mobile device for a successful reprogramming, and care should be taken to avoid the risk of data loss or damage to the device during the update.

REFERENCES

[1] O. Lutskyi, "Tactics of using unmanned aerial vehicles in the protection of the state border: a textbook," Khmelnytskyi: NADPSU Publishing House, 2023, 164 p.

[2] D. Shamanov and A. Sorokin, "Analysis of modern methods of electronic warfare," Kharkiv National University of Radio Electronics, Control, Navigation and Communication Systems, no. 1, pp. 211-214, Kharkiv, Ukraine, 2024, doi: 10.26906/SUNZ.2024.1.211.

[3] I. Mayboroda, K. Vlasov, and M. Glushchenko, "Application and Prospects for the Development of Mobile Electronic Intelligence Means of the Tactical Link of the Security and Defense Forces of Ukraine," National Academy of the National Guard of Ukraine, Journal "Honor and Law", vol. 2, no. 89, 2024, doi: 10.33405/2078-7480/2024/2/89/309207.

[4] S. Mosov, "Swarming of Military Drones: Realities and Prospects," Institute of Public Administration and Civil Defense Research, no. 1(80), pp. 77-86, 2024, [Online]. Available: https://doi.org/10.33099/2304-2745/2024-1-80/77-86.

[5] O. Karatanov, O. Ustymenko, M. Jena, E. Bova, and V. Kalashnikova, "The use of swarm intelligence algorithms in the design of control systems for groups of unmanned aerial vehicles," Young scientist, vol. 10, no. 98, pp. 98-103, 2021, [Online]. Available: https://doi.org/10.32839/2304-5809/2021-10-98-24.

[6] K. Klyarskyi, "Quadrocopter control system: bachelor's thesis," 151 Automation and computer-integrated technologies, Kyiv, 2024, 100 p.

[7] G. Howell, J. M. Franklin, V. Sritapan, M. P. Souppaya, and K. Scarfone, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) NIST SP 800-124r2, 51 p., May 2023, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-124r2.

[8] F. Mahfoudhi, A. K. Sultania, and J. Famaey, "Over-the-Air Firmware Updates for Constrained NB-IoT Devices," Sensors, vol. 22, no. 19, p. 7572, 2022, doi: 10.3390/s22197572.

[9] P. Hou et al., "Distributed DRL-Based Intelligent Over-the-Air Computation in Unmanned Aerial Vehicle Swarm-Assisted Intelligent Transportation System," IEEE Internet of Things Journal, vol. 11, no. 21, pp. 34048-34054, 2024, doi: 10.1109/JIOT.2024.3418882.

[10] M. Sadiku, N. Akujuobi, and O. Cajetan, "Software-defined radio: A brief overview," Potentials, IEEE, vol. 23, pp. 14-15, 2004, doi: 10.1109/MP.2004.1343223.

[11] B. R. Mahafza, S. C. Winton, and A. Z. Elsherbeni, "Handbook of Radar Signal Analysis," 1st ed., Chapman and Hall/CRC, 2021, 706 p., doi: 10.1201/9781315161402.

[12] Planeta hobby, "Tips for managing FPV frequencies," [Online]. Available: https://modelistam.com.ua/ua/sovety-upravleniyu-chastotami-a-300/.

[13] "RSSI verstehen: Eine Schlüsselmetrik für FPV-Systeme mit großer Reichweite DJI-Systeme im Vergleich zu analogen Systemen," [Online]. Available: https://fpvracingdrone.de/fpv/rssi-sender-empfaenger-grosse-reichweite-fpv/.

[14] "How to avoid intermodulation distortion and ensure a stable FPV video signal," [Online]. Available: https://fpvua.org/threads/jak-uniknuti-intermoduljacijnix-spotvoren-i-zabezpechiti-stabilnij-videosignal-fpv.361/.

[15] "The role of satellite interference in failures in modern communications," [Online]. Available: https://www.szmidjammer.com/uk/blog/satellite-jammer/.

[16] V. Chmeliov, "Radio control systems. Home control work, Study guide for students majoring in 172 'Electronic Communications and Radio Engineering'," Igor Sikorsky Kyiv Polytechnic Institute, Kyiv: Igor Sikorsky Kyiv Polytechnic Institute, 2023, 24 p.

[17] V. Savko, "Development of an ARI stand for machine-to-machine interaction: diploma thesis," Bachelor's degree: 121 Software Engineering, Kyiv, 2021, 75 p.

[18] P. Holodiaieva, "Algorithm for estimating the UAV motion parameters based on the Kalman filter: diploma thesis," Bachelor's degree: 172 Telecommunications and Radio Engineering, Kyiv, 2023, 78 p.

[19] M. Yatsymon, "Methods for increasing the protection of the control radio channel from interception by unmanned aerial vehicles: graduation qualification work: 125 'Cybersecurity'," National University "Chernihiv Polytechnic", Department of Cybersecurity and Mathematical Modeling, Chernihiv, 2023, 71 p.

[20] V. Pavlenko, "Investigation of the influence of intentional interference on UAV communication channels: diploma thesis," Bachelor's degree: 172 Telecommunications and Radio Engineering, 2023, 51 p.

[21] X. Jiang, L. Jiang, Y. Xiao, and C. Xiao, "Design of Wireless Communication System Based on nRF24L01," Advanced Materials Research, vol. 945-949, pp. 1756-1759, 2014, doi: 10.4028/www.scientific.net/AMR.945-949.1756.

[22] H. Wang, C. Li, and F. Wu, "Design and Implementation of Broad-Band Jamming Signal Source for GPS," Proceedings of the 2016 International Conference on Computer and Information Technology Applications, pp. 68-73, 2016, ISSN 2352-538X, doi: 10.2991/iccita-16.2016.13.

[23] J. Li, "Working principle and application analysis of phase-locked loop," Applied and Computational Engineering, vol. 11, pp. 174-180, 2023, doi: 10.54254/2755-2721/11/20230228.

[24] D. Debojyoti, N. R. Sivaraaj, and M. Abdul, "Exploring the Landscape of Phase-Locked Loop Architectures: A Comprehensive Review," IEEE Access, pp. 1-1, 2024, doi: 10.1109/ACCESS.2024.3446393.