Security Analysis of a Swarm of Drones Resisting Attacks by Intruders*

Vitaly A. Dovgal[1][0000-0003-4181-8776] and Dmitry V. Dovgal[2][0000-0001-8880-7308]

[1] Maykop State Technological University, Maykop, Russia
vdovgal@mkgtu.ru
[2] Don State Technical University, Rostov-on-Don
lanayamann@gmail.com

Abstract. Currently, to perform a certain task (for example, a search operation), unmanned aerial vehicles have been combined into an organized group, which can be called a swarm. Naturally, such an information system is of interest to hackers who are trying to use drones for malicious purposes. The number of attacks increases with the increase in the active introduction of a flock of drones in their practical application. The probability and frequency of these attacks are high, and their impact can be very dangerous and the consequences devastating. Therefore, protective and preventive countermeasures are urgently needed to ensure conditions that reduce the impact of intruders on the drone system to a minimum and detect eavesdropping devices and unauthorized connections. The purpose of this study is to analyze and review the threats used in cyber-attacks on a swarm of unmanned aerial vehicles, as well as measures to counter these attacks. The article discusses the architecture of drones and the types of connections for their interaction in a flock analyzes existing threats and vulnerabilities of drones. Special attention is paid to such types of illegal entry into the system of interacting drones as hacking and intrusion. The most accessible methods of hacking and intrusion by intruders are considered, as well as methods and mechanisms for protecting data processed in systems, including intrusion detection systems, neural networks, and fuzzy rule-based systems.

Keywords: Unmanned Aerial Vehicle, Security, Threats and Vulnerabilities, Information Attacks, Hacking Methods, Protection Against Hacking.

1 Introduction

Currently, unmanned aerial vehicles (UAVs) are increasingly used to perform a certain task (for example, a search operation) not alone, but as part of an organized group, which can be called a swarm (or flock) [1]. Remote control of a swarm of UAVs is usually carried out using a ground station (GS), which allows you to perform a fully autonomous flight. A smartphone connected to a mobile network can be one of the options for implementing a GS. From the point of view of security, a swarm of drones, as an object of a wireless computer network, will be subjected to various attacks by intruders. These attacks can have serious consequences, including commercial and non-commercial losses. In this context, there is a lack of proper understanding of how attackers perform their attacks and capture a drone to gain control over it. As a rule, compromising a group of drones is carried out for malicious purposes. Therefore, there is a need to detect attacks and prevent them from causing any damage. This article will provide an overview of possible attacks by an attacker and possible ways to counter them.

2 The Architecture of Drones and Types of Connections for their Interaction in the Swarm

Typically, the UAV architecture consists of three main elements [2, 3]:

1. the actual UAV (unmanned aerial vehicle), controlled by the central processor of the drone;
2. a ground station (GS) located on a ground facility that provides human operators with the ability to control and/or monitor the flock while they are working remotely. Stations are classified according to the size, type, and tasks of unmanned aerial vehicles;
3. communication data-link (CDL) – a wireless channel used to control the information flow between the swarm drones and the ground station. Control of unmanned aerial vehicles can be classified by their distance from the GS:

   - visual line of sight distance: control signals are transmitted and received using radio waves;
   - the distance beyond the line of sight: control of unmanned aerial vehicles is carried out using satellite communications.

There are four main types of communication with drones:

1. drone-to-drone (D2D) is a non-standardized type of communication that can be considered as a peer-to-peer (P2P) network that is vulnerable to various types of P2P attacks, including interference. For example, distributed denial of service (DDoS) and Sybil attack (a network attack in which one of the nodes may have multiple IDs, which disrupts the system);
2. drone-ground station (D2GS) – communication using standardized industrial wireless protocols (Bluetooth and Wi-Fi 802.11, including 2.4 GHz and 5 GHz). Their wide popularity makes such communication public and insecure (even when using one-factor authentication, which can be easily overcome by an intruder). Communications become vulnerable to passive (eavesdropping) and active (man-in-the-middle) attacks;

3. drone-network (D2N) – communication that allows you to choose a network based on the required level of security, which is very important to ensure when using such wireless communication networks;
4. drone-satellite (D2S) – communication that allows you to use the transfer of coordinates of aircraft in real-time through the global positioning system (GPS). Using the coordinates of the earth's surface allows you to track the location of the drone and develop a control action (for example, to call the drone back to the source station if it went beyond the control line or the line of sight). Satellite communications are considered reliable and secure. However, this type of communication is quite expensive, and also requires special maintenance requirements.

Figure 1 shows the structure of communication as drones with each other and with the ground station.

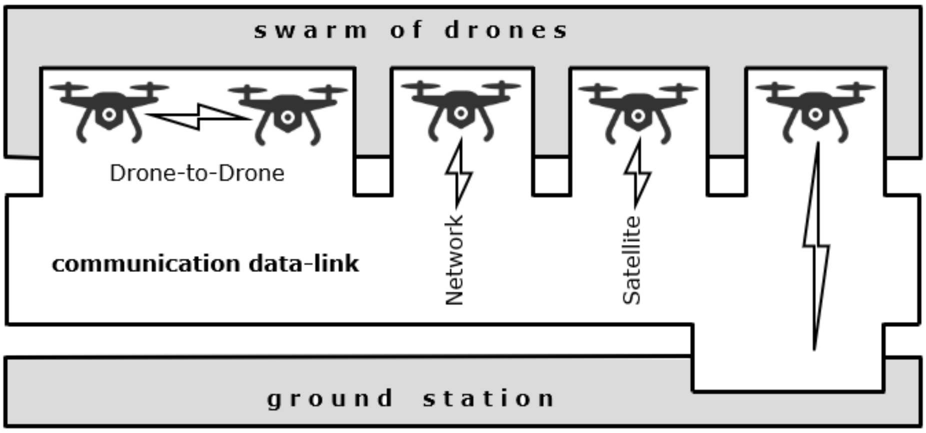

Fig. 1. The architecture of drones and types of connections for their interaction in the swarm.

3 The Types of UAV

All unmanned aerial vehicles are drones, but not all drones are unmanned aerial vehicles. Consider the difference between these categories of aircraft.

Drones

Drones are usually referred to as aircraft that use remote (Autonomous) control. Similarly, drones can be called other similar vehicles (submarines, ground-based Autonomous vehicles, etc.). According to the flying mechanisms used, drones can be classified as follows: [4]

a) multi-rotor drones (rotary drones) – aircraft with vertical take-off and landing, having the properties of maneuverability and hovering over a fixed point on the Earth's surface. The latter property allows you to provide constant cellular coverage over certain areas, as well as act as base stations, providing high accuracy of geolocation. Their disadvantages: limited mobility and high power consumption;

b) fixed-wing unmanned aerial vehicles – aircraft that move in the air like an airplane, using the lifting force due to the incoming flow. This way of moving makes them more energy-efficient than multi-rotor drones. Disadvantages: the need for a runway for takeoff and landing and the inability to hover over a fixed point of space, high cost;

c) unmanned aerial vehicles with a hybrid wing – similar to the previous drone with the ability to rotate the wing, which allows the aircraft to quickly reach the target, gliding through the air and hovering with the help of four rotors.

Unmanned aerial vehicle

Such an aircraft can fly remotely/autonomously using a controller, mobile phone, computer, or even tablet. Advantages: the ability to work over long distances with reliable live data transmission. Usually, UAVs are controlled by remote control with the help of a pilot; remote-controlled control (the mission is performed automatically but with the possibility of operator intervention); full autonomous flight.

Unmanned aircraft systems (UAS)

This group includes both UAVs and drones, as well as the operators who operate them. A UAV is a type of UAS, as it refers to a controlled vehicle or aircraft.

Remotely piloted aircraft

A remotely piloted aircraft that requires intensive skills and training over a long time (several years) to manage these complex flights.

4 Existing Threats and Vulnerabilities Drones

UAVs and drones are considered promising objects that have vital threats to information security. Many UAVs have serious design flaws, and most of them are designed without the use of a wireless security system and video encryption.

Due to the ever-increasing number of drones in the air, it is necessary to take measures to prevent incidents that may occur as a result of cyber-attacks. The level of attacks will continue to increase, and manufacturers, as well as governments, must make a collective effort to protect these systems from attacks. To ensure the safety of these devices and the civilians who use them, it is necessary to significantly increase the level of protection of the drone software from external intrusion. Let's look at various hacking strategies that can be used by hackers to gain control of UAVs.

Hacking – illegal entry into another system or network. Wireless attacks are the most common form of hacking and compromising the system, leading to the loss of control over the drone by its rightful owner. The most available methods of hacking are:

a) password theft implemented using special software tools, such as dictionary attacks (scanning open ports and using a list of common words from the dictionary to perform the attack), brute force attacks, and statistical methods such as Aircrack-NG [5];

b) using the application Wireshark – a reliable tool for analyzing and capturing packets for wireless networks, which also allows you to gain access to the client system and subsequent control over it [6];

c) man-in-the-middle attacks (MITM) – an attack in which an attacker gains control of confidential data by stealthily changing the communication channel between two parties [7];
e) Trojan horse virus – a malicious program or software that tracks network traffic and causes harmful consequences by destroying files and damaging hard drives in the system [8];
e) distributed denial of service attacks (DDoS) – a large-scale intrusion method performed by a host source that causes harmful consequences for legitimate users, delaying the provision of services requested by them [9]. As a result of the attack, either the system is completely disabled, or its system resources (computing power and bandwidth) are depleted.

5 Protection Against Hacking

There are many ways to secure drones by preventing threats at the root or identifying them and taking appropriate action when they occur. However, no system is completely secure due to its inherent operating system flaws, which can lead to vulnerabilities. Most common attacks are usually caused by external agents. This section provides an overview of some existing solutions to improve the safety of drones.

Encryption

Encryption is a simple method of protecting confidential data in systems that allows access only to legitimate users [10]. This method acts as a barrier against unwanted actions, denying access to protected resources and facilitating the safe transfer of confidential information.

To successfully resist brute-force attacks, you can strengthen encryption by increasing the key length. Also, to prevent hacking, we recommend hiding access points by disabling the system's service set identifier (SSID) and allowing access to systems with familiar MAC addresses. Sometimes fake MAC addresses also allow hackers to join the network. In the case of UAVs, the password can be used to verify the authenticity of messages transmitted between the UAV and the operator.

Protection against DDoS attacks

There are several mechanisms to prevent DDoS attacks:

- reactive mechanisms ("early warning systems") that use a mechanism to identify an attack at its source to prevent damage [11];
- preventive mechanisms that minimize the possibility of an attack by taking corrective measures. Regular scanning with antivirus scanners, firewalls, patches, and antivirus programs, and maintaining appropriate protocols with sensors and filtering mechanisms help control abnormal activity. This includes logging normal system behavior and constantly checking for strange or specific behavior. To determine the size of the anomaly, a threshold value is set.

DDoS attacks are also prevented by signature detection, which uses a database of well-known attacks to compare and identify incoming attacks. The disadvantage of this method is that it is not possible to identify any new attacks on the system. Attempts to protect the system before an attack are extremely important because they reduce the likelihood of a potential DDoS attack.

The hybrid protection system uses a combination of preventive and reactive methods as a countermeasure against DDoS attacks.

Intrusion detection systems (IDS)

Intrusion is a method of unauthorized entry or compromise of system resources without the consent of the rightful owner. Intrusion detection is a way to monitor and detect signs of abnormal activity.

Intrusion detection systems are a software package that checks the system behavior for anomalies [12]. IDS are security tools, but they do not provide preventive actions to protect the system. There are two types of IDs: misuse IDs and anomaly IDs.

Misuse of IDS deals with pre-defined attack signatures that take advantage of security loopholes. Such signatures are well known before an attack and are used to check incoming patterns for their virulent nature.

The IDS anomaly uses regular system performance to check its behavior and generate relevant statistics. If there is a deviation from normal usage performance, this behavior is noted by the mechanism in IDS.

IDS identifies incoming traffic and determines whether it should be protected or not. It uses three types of information:

1. long-term information related to the database construction methods used in detecting attacks;
2. configuration information that depends on the current state of the system;
3. audit information reflecting the situation and circumstances of the system functioning.

Neural networks in intrusion detection systems

Classification functions used by neural networks can perform intrusion detection [13]. Neural networks identify the pattern or signature of the input signal and place it in classes, respectively, at the output. Neural networks used in IDS are classified as follows:

a) multi-layer direct neural networks consisting of a hidden layer between the input and output layers;
b) self-organizing Kohonen maps that form a mapping from the entrance to the clusters. The detection process is accelerated using a neural network, as it can recognize the features of past intrusions.

Fuzzy rule-based systems in IDS.

Fuzzy logic is a method that uses approximation methods instead of fixed values. In binary systems, either 0 or 1 is used, but using fuzzy logic, we can get ranges that lie between 0 and 1. This provides partial or intermediate values and, therefore, a fuzzy database can be formed [14]. These systems are flexible and take approximate values into account. Any valid set of data defined based on input and output values can be converted to a fuzzy system.

Fuzzy logic allows for errors or uncertainty and provides a low-cost solution in the system. This provides significant advantages over other soft computing methods in intrusion detection. It detects abnormal activity in the system and formalizes strategies to eliminate it accordingly. The fuzzy system used for intrusion detection has the following stages:

a) creating a fuzzy rule strategy;
b) decision-making module using a fuzzy rule;
c) the appropriate classification of the input data.

Using approximate data, *if-then* rules can be formed using expert knowledge. The disadvantage of this method is that the number of *if-then* rules increases rapidly as the data set increases. In neural networks, training is required, but in fuzzy systems, rules are formed to get conclusions related to the data set.

Fig.2 shows the classification of methods of protection against hacking.

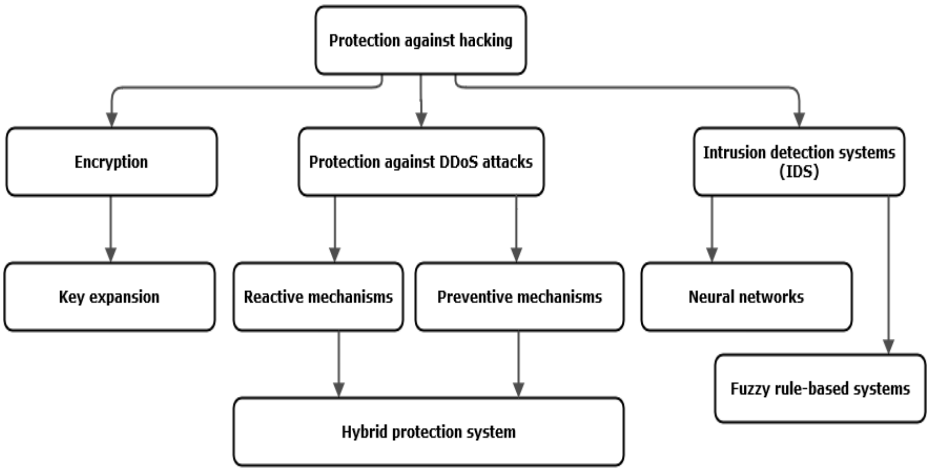

Fig. 2. Classification of methods of protection against hacking.

6 Conclusions

This study addressed the importance of ensuring privacy related to unmanned aerial vehicles to prevent the disclosure and use of data obtained by drones. The article outlines various strategies for hacking a swarm of drones and offers various security suggestions and recommendations to ensure the safer use of unmanned aerial vehicles and drones. Among the proposed solutions to protect against such attacks, various methods are proposed, including neural networks and intrusion prevention systems based on fuzzy logic.

References

1. Dovgal, V.A., Dovgal, D.V.: Model of the Interaction of Analyzing Fog-Cloud Computing for Processing Information about the Position of Unmanned Aerial Vehicles. Autumn Mathematical Readings in Adygea. Materials of the III International scientific conference. Pp. 149-154. (2019). (In Russian)
2. Altawy, R., Youssef, A.M.: Security, Privacy, and Safety Aspects of Civilian Drones: a Survey, ACM Trans. Cyber-Phys. Syst. 1 (2) (2017) URL: https://dl.acm.org/doi/10.1145/3001836.
3. Chen, M., Challita, U., Saad, W., Yin C., Debbah, M.: Machine Learning for Wireless Networks with Artificial Intelligence: a Tutorial on Neural Networks, arXiv Preprint arXiv:1710.02913 (2017).
4. Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L.G., Garcia-Rodriguez, A., Yuan, J.: Survey on UAV Cellular Communications: Practical Aspects, Standardization Advancements, Regulation, and Security Challenges, arXiv Preprint arXiv:1809.01752 (2018) https://arxiv.org/abs/1809.01752.
5. Albitov, A. M.-H.: Estimation of Security of a Wireless Wi-Fi Network with the Help of Specialized Software "AIRCRACK-NG". Current Issues of Operation of Security Systems and Secure Telecommunications Systems. Collection of materials of the all-Russian scientific and practical conference. Pp. 273-275. (2018). (In Russian)
6. Gladkikh, A.M.: Main Methods of Network Traffic Analysis. Questions of Science and Education. No. 19 (103). pp. 23-28. (2020). (In Russian)
7. Dovgal, V.A., Dovgal, D.V.: Detection and Prevention the Man in the Middle Attack in the Foggy Layer of a Swarm of Drones. Bulletin of the Adygeya State University. Series: Natural-mathematical and technical Sciences. Issue 2 (261) Pp. 53-59. (2020). (In Russian)
8. Palaeva, L.V., Khafizov, A.M., Gilyazetdinova, A.M., Vakhitova, A.R., Davydova, K.N., Sirotina, E.R.: The Main Types of Cyber-Attacks on Automated Control Systems of Technological Process and Means of Protection Against Its. Fundamental research. No. 10-3. pp. 507-511. (2017). (In Russian)
9. Ibragimova, L.M.: DDOS Attacks: Essence, Classification, Threats, and Methods of Struggle. From Scientific Ideas to Business Development Strategy. Collection of articles-presentations of research papers of students, masters, postgraduates, young scientists-participants of the International Interuniversity Student conference on national security as the basis of competitiveness and economic growth of the country. Pp. 82-87. (2019). (In Russian)
10. Selikhov, V.A.: Ensuring the Safety of UAV Flights. The Synergy of Sciences. No. 22. P. 830-836. (2018). (In Russian)
11. Petrenko, S.A., Petrenko, A.S., Makoveychuk, K.A., Makoveychuk, Y.T.: Early Warning Systems for Cyber-Attacks Based on BIG DATA Technologies. Financial, economic, and information support of innovative development of the region. Collection of materials of the all-Russian scientific and practical conference. Dedicated to the 100th anniversary of the V.I. Vernadsky Crimean Federal University. Responsible editor A.V. Olifirov. Pp. 431-434. (2018) (In Russian)
12. Ryapolova, E.I., Tsvetkova, K.E.: Analysis of Anomaly Detection Systems and Hybrid Intrusion Detection Systems. Problems and prospects of introduction of innovative telecommunication technologies. Collection of materials of the VI International scientific and practical full-time and correspondence conference. Editor-in-chief: A.V. Kiryakova. Pp. 130-142. (2020). (In Russian)
13. Bukhanov, D.G., Polyakov, V.M., Smakaev, A.V.: Determining the State of a Computer Network Based on the Use of Neural Networks. Bulletin of the Belgorod state technological University named after V. G. Shukhov. No. 7. Pp. 157-162. (2017). (In Russian)
14. Nauck, D. and Rudolf, K. A.: Neuro-Fuzzy Method to Learn Fuzzy Classification Rules from Data. Fuzzy Sets Syst; 89: 277–288. (1997).