Analysis of Communication Channels for the Organization of Control and Interaction of UAVs from the Security Viewpoint

Elena Basan[1], Olga Peskova[1] and Maria Lapina[2]

[1] *Southern Federal University, Chekhov St., 2, Taganrog, 347922, Russia*
[2] *North Caucasus Federal University, Pushkina St., 1, Stavropol, 355017, Russia*

Abstract

This article considers the issues of increasing the level of security of wireless communication channels between UAVs. The topic is quite relevant, since UAVs can be used to solve critical tasks, such as search operations, reconnaissance, and relaying communications. At the same time, wireless communication channels are not physically protected, and their security can easily be compromised. The article also discusses the main vulnerabilities of communication channels for UAVs, attacks, and threats to information security. Possibilities of increasing the level of security of UAV communication channels are considered. The methods and developments suggested on this topic by the authors are briefly presented.

Keywords

UAVs, vulnerabilities, threats, attacks, cryptography, attack detection, communication channels, modulation

1. Introduction

Recent years can be characterized by an active expansion of the application areas of unmanned aerial vehicles (UAVs) both for military and civil purposes; therefore, information security issues are becoming more and more urgent, and above all, no less urgent are the problems of the protection of the most vulnerable components of UAVs, and data transmission channels.

The main goal of the study is to analyze the technologies used to organize communication channels of various types, as well as to analyze the information security problems typical for them.

2. Analysis of UAV control methods

As a rule, any architecture using a UAV includes three control elements [1]:

- The UAV itself, and, in particular, the flight controller, which is defined as the central processor;
- Ground control station (GCS) which provides operators with the necessary capabilities to control and/or monitor the UAV;
- Data transmission channels, i.e. wireless channels used to control the information flow between UAVs and GCSs.

Accordingly, the organization of communication channels can be divided into 4 main types:

1. UAV - UAV (D2D). This type of communication is not standardized [2]. In most cases, D2D communications can be modeled as Peer-to-Peer (P2P) communications, which makes such communications vulnerable to various types of attacks typical of P2P, including noise, distributed denial of service (D-DoS), and Sibyl attack.

SibDATA 2021: The 2nd Siberian Scientific Workshop on Data Analysis Technologies with Applications 2021, June 25, 2021, Krasnoyarsk, Russia
EMAIL: ele-barannik (E. Basan)
ORCID: 0000-0001-6127-4484 (E. Basan); 0000-0001-8117-9142 (M. Lapina)

2. UAV - GCS (D2GS). This type of communication is based on the already known and standardized industrial protocols based on wireless communication such as Bluetooth and Wi-Fi 802.11. However, most ground-to-ground connections are public and insecure, especially when using single-factor authentication, which can be easily attacked, making them vulnerable to passive (traffic interception, infrastructure analysis) and active (man-in-the-middle, denial of service) attacks.
3. UAV - UAV group (D2N). This type of communication already allows one to select a network based on the required level of security. It can also include cellular communication, which means using 3GHz, 4GHz, 4G (LTE), and 5GHz.
4. UAV - Satellite (D2S). This is the type of communication required to send coordinates in real-time via the Global Positioning System (GPS), allowing any UAV to return to its original station in the case when it goes out of the line of sight. Satellite communications are considered relatively safe, although vulnerable to attacks such as GPS signal spoofing, etc.

Control over UAVs can be carried out in three main ways [3]:

- using a remote control, where all decisions are made by a remote operator;
- remote controlled control: with the ability to start and execute the given autonomy, at the same time allowing human intervention if necessary;
- complete autonomous control: UAVs can make all necessary decisions without the need for any human intervention.

On the one hand, UAVs must exchange critical information with various entities, such as operators, nearby aircraft and air traffic controllers to ensure safe, reliable, and efficient flight operations. This type of communication is known as Controlled and Non-Payload Communication (CNPC) [4]. On the other hand, depending on the mission, it may be necessary to transmit and/or receive mission-related data in a timely manner, such as aerial photographs, high-speed video, and data packets for relaying to/from various ground objects such as UAV operators, final users or ground gateways. For this, communication with the payload is used. Specific communication and spectrum requirements are generally different for CNPC and for payload transmission. The 3rd Generation Partnership Project (3GPP) consortium defined the communication requirements for these two types of channels [5]. CNPC usually has a low data transfer rate but rather stringent requirements for high reliability and low latency. Since the loss of a CNPC channel can lead to catastrophic consequences, the International Civil Aviation Organization ICAO states that CNPC channels for UAVs must operate in a protected aviation spectrum [6].

In [7] two methodologies for estimating the spectrum requirements for CNPC are presented. For both UA density methodologies, a terrestrial line-of-sight (LOS) spectrum requirement of 34 MHz is determined. For a non-line-of-sight (BLOS) satellite, the spectrum requirement ranges from 46 MHz to 56 MHz, depending on the type of the satellite system used (spot beam or regional beam).

Depending on the functions performed by the UAV, communication can be organized in two ways to improve reliability. As a rule, at least two communication systems are located onboard the UAV: duplex / half-duplex equipment for transmitting command-telemetric information and a simplex system for transmitting payload information. At the same time, on the one hand, an increase in the data transmission channels increases the reliability and resilience of the communication lines, but on the other hand, it provides a potential adversary with more opportunities to make attacks.

Let us consider, in particular, the features of using of satellite communications for the organization of communication between GCS and UAV. Satellites can be used to relay communications if the UAVs and GCSs are separated by significant distances, for example, if the UAV is over the ocean or in remote areas where the coverage of the terrestrial network is absent. In addition, satellite signals can also be used to navigate and localize UAVs. WRC 2015 approved the conditional use of satellite frequencies in the Ku/Ka-band to connect UAVs to satellites, and some satellite companies, such as Inmarsat, have launched satellite communication services for unmanned aerial vehicles [8].

Nevertheless, there are several problems which arise in the case of organizing satellite communication between GCS and the UAV. First, the loss and delay of the signal is very significant due to large distances between the satellite and the UAV / ground stations, which are located at low

altitudes, which is unacceptable for the transmission of control and telemetry data. Second, unmanned aerial vehicles usually have strict size, weight, and power constraints, and may not be able to carry heavy, bulky, and energy-intensive satellite communication equipment. Third, high operating costs of satellite communications also make it difficult to use it widely for large groups of UAVs. Figure 1 shows a picture of possible control and communication channels with a UAV.

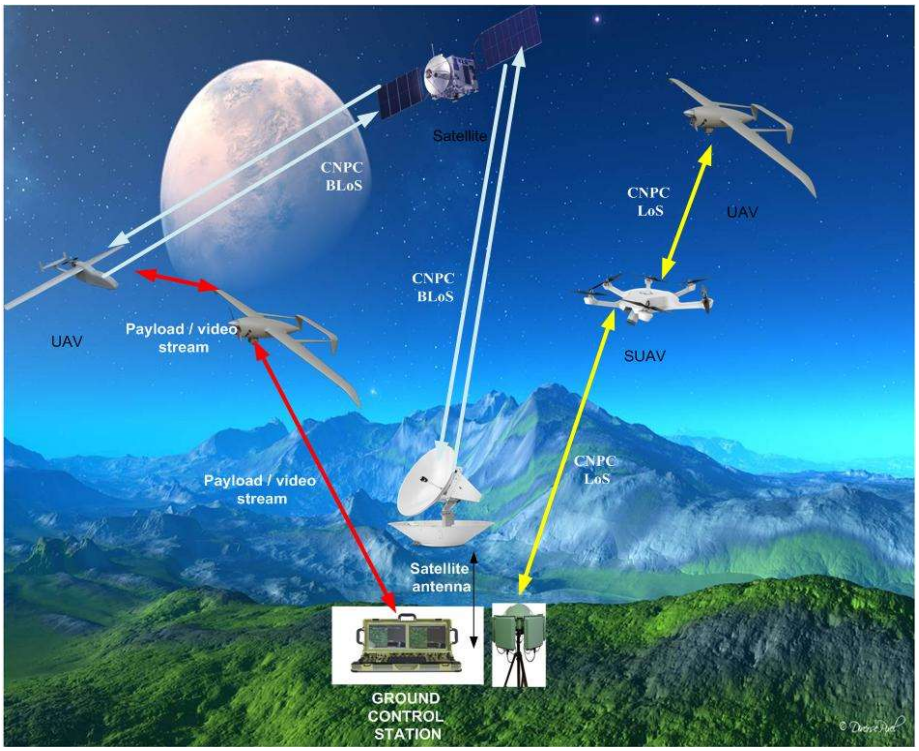

Figure 1: UAV communication and control channels

The next way of organizing communication, which can serve both for communication between GCS and the UAV and for communication between the UAV and the UAV, is an ad-hoc network, i.e. a decentralized wireless network with no permanent structure. Its variation in the Mobile ad-hoc network (MANET) is a dynamically self-organizing network which does not have a permanent infrastructure, which implements peer-to-peer communication between mobile devices through wireless communication lines, using, for example, IEEE 802.11 a / b / g / n. Each device in MANET can move randomly in time; as a result, its communication conditions with other devices may change frequently. In addition, in order to support communication between two remote sites, some other sites between them must help to forward data through relaying, resulting in higher power consumption, low spectrum efficiency, and long end-to-end latency. Flying ad hoc network (FANET) is a variant of MANET for supporting communication between unmanned aerial vehicles in 3D networks [9]. The topology or configuration of FANET for a UAV can take a different form: full mesh, ring, star, or even bus, depending on the application scenario.

In [10], the issue of organizing a communication channel between several UAVs and a ground control point is considered. In this topology, each slave UAV transmits its data to the leader of the UAV group, and the latter transmits the information to the ground control panel. According to the research results, it is noted that the statistics of errors in wireless channels between UAVs change depending on changes in the distance between UAVs.

While FANET is a robust and flexible architecture to support UAV communications in a small network, it cannot generally provide a scalable solution for large UAVs deployed over a large area due to the complexities associated with implementing a robust routing protocol and it has a number of features in terms of radio wave propagation.

Recently, interest has increased in the use of the existing cellular communication networks, as well as future generation networks to ensure the possibility of terrestrial communication of UAVs [11], due to almost ubiquitous coverage of the cellular network throughout the world, as well as its high-

speed optical backhaul and advanced communication technologies, which can potentially meet the requirements of both CNPC and payload, regardless of the density of the UAVs and their distance from the corresponding ground nodes.

In [12] the authors discuss the issues of building a UAV network using LTE (Long Term Evolution) technology, a standard for wireless high-speed data transmission in the networks of mobile operators. At the same time, an unmanned aerial system is considered, which includes a UAV, an antenna-feeder facility, and a ground control point. The authors consider the problem of defining upper layer protocol sets for the Radio Monitoring and Non-Payload Communication (CNPC) Standard, which is being developed within the Radio Technical Commission for Aeronautics (RTCA) [13, 14]. This standard only describes the radio frequency (RF) transmission methods and the physical layer; therefore, it is necessary to select and configure the upper layer protocols and define the network architecture of CNPC. The US National Space Agency (NASA) is considering IEEE 802.16 based upper-layer protocols and the CNPC network architecture, but the authors of the article consider the application of the upper layer protocols and the LTE based CNPC network architecture [15, 16]. The frequency for CNPC was discussed at the World Radio Conference (WRC) of the International Telecommunication Union, Radiocommunication (ITU-R), and the frequency band 5 030-5 091 MHz was allocated to CNPC at WRC-12 [17, 18]. The LTE upper-layer protocols for the wireless interface consist of Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), and Radio Resource Control (RRC).

To ensure the security of this type of connection, VPN (Virtual Private Network) technologies and a group of IPSec protocols can be used. However, the LTE standard is characterized by many vulnerabilities which can be revealed through the following attacks:

- interception of personal user identifiers MSISDN, IMSI;
- location determination;
- man-in-the-middle attacks for unencrypted traffic (interception of access to unprotected mail, visited sites, etc.);
- interception of SMS messages;
- listening to VoLTE calls by intercepting packets;
- creating a session on behalf of the subscriber for the purpose of fraud.
- denial of service attacks on the subscriber, which cause the loss of user data transmission, and for VoLTE networks - interruption of calls;
- denial of service attacks on equipment which result in network outages.

The disadvantages of using open communication protocols are:

- low information security of the communication channel (cryptographic strength);
- low imitation resistance (resistance to imitation noise, which has the same structure as a useful signal, which makes it difficult for detection);
- lack of hidden and noise-immune modes of operation.

Thus, the study defines the main architectures which can be used to build communication networks with UAVs. The collected data will be used to achieve the following goals: development of a UAV detection system, development of a system for creating false images of a UAV group.

3. UAV Control and communication vulnerabilities

Many unmanned aerial vehicles have serious design flaws, and most of them are designed without wireless protection and encryption of transmitted data [19].

Spoofing vulnerability: The analysis of the configuration of multi-rotor UAVs and flight controllers revealed many deficiencies. They are associated with telemetry streaming channels over serial ports, especially due to the lack of encryption [20, 21]. Our experiments show that using GPS spoofing, information can easily be captured or altered. This vulnerability in the data link allows data to be intercepted and tampered with, giving full control over the UAV.

Vulnerability to malware infection: Communication protocols are used when establishing a control channel with a UAV for enabling remote control of unmanned aerial vehicles. However, their use turned out to be unsafe [22,23]. A potential adversary can create a TCP payload, inject it into the UAV's memory, which makes it possible to covertly install malware into systems operating at ground stations.

Vulnerability to interference with the communication channel and data interception: Telemetry data transmission channels are used to monitor the environment and objects and implemented through a wireless data transmission medium [24], which makes them vulnerable to various threats. These include data interception, malicious data injection, and alteration of predefined flight paths. This makes it possible to inject and deploy many infected digital files (video, images) from a UAV to the ground station [25]. Another vulnerability was discovered and related to the UAV communication module, which uses wireless communication to exchange data and commands with the ground station [26].

4. Experiments

The members of our team working on the UAV security project carried out a number of experiments to identify vulnerabilities in the communication and control channels of the UAV.

The study and analysis of the scenarios of active, passive, and multi-stage attacks for an intelligent group control system for UAVs were carried out, and based on them a template for describing attacks and general scenarios for influencing the information system of a UAV was proposed, and probable attacks through communication channels (deauthentication and connection, eavesdropping, Blueprinting, Replay, Interception of "handshake", brute-force and others) were described [27].

The analysis and study of the algorithms and methods of influencing the UAV information system through communication channels were performed, including the study of the Data Distribution Service, Micro Air Vehicle Link, MAVLink protocols. Field experiments were carried out on the UAV navigation system, built using the GPS technology. During these experiments various types of attacks were implemented, leading to misinformation, return or forced landing of the UAV. The studies were also carried out on the required power, and requirements for the content of the generated signal. The characteristics of determining the fact of an ongoing GPS spoofing attack were also proposed [28].

A system for the formation of a false idea of a UAV based on the use of a radio frequency channel is proposed, which is based on imitating the presence of a large group of UAVs around a trusted UAV object, which simulates communication over a wireless communication channel and at the same time deliberately uses weak security measures (weak passwords, cryptographic keys), which is necessary to draw the enemy's attention to false UAVs instead of the trusted ones [29].

5. Conclusion

Thus, in the course of the study, a detailed analysis of the UAV control methods was made, various technologies used to ensure communication and control of UAVs in various interaction schemes were presented, their vulnerabilities and possible attacks were considered. The experiments carried out during the research were described which showed the real threat from the vulnerabilities. This can make it possible to develop an integrated UAV protection system both in single and group versions.

6. References

[1] M. Marshall, R. K. Barnhart, S. B. Hottman, E. Shappee, M. T. Most, Introduction to unmanned aircraft systems. 1st edit. CRC Press. Boca Raton 2016, doi:10.1201/b11202.

[2] M. Chen, U. Challita, W. Saad, C. Yin, M. Debbah,Artificial Neural Networks-Based Machine Learning for Wireless Networks, in: IEEE Communications Surveys & Tutorials, volume 21(4), 2019, pp. 3039–3071. doi: 10.1109/COMST.2019.2926625.

[3] J. Eggers, M. Draper, Multi-UAV control for tactical reconnaissance and close air support missions: operator perspectives and design challenges, in: Proceedings NATO RTO Human Factors and Medicine Symp, Biarritz, France, 2006, pp. 2006–2011.
[4] D.C. Iannicca, J. A. Ishac, K. Shalkhauser, Research Center. Control and Non-Payload Communications (CNPC) Prototype Radio – Generation 2 Security Flight Test Report. National Aeronautics and Space Administration Glenn Research Center Cleveland, Ohio, 2015.
[5] Technical specification group radio access network: study on enhanced LTE support for aerial vehicles, volume 15.0.0, 2017, URL: https://standards.aw-drones.eu/standard/652, last accessed 2021/03/21.
[6] R. J. Kerczewski, J. D. Wilson, W. D. Bishop Frequency spectrum for integration of unmanned aircraft, in: 32nd Digital Avionics Systems Conference (DASC), IEEE, East Syracuse, NY, USA, 2013, pp. 651–659. doi: 10.1109/DASC.2013.6712625.
[7] Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace. International Telecommunication Union, Tech. Rep. M.2171, M Series Mobile, radiodetermination, amateur and related satellites services. Electronic Publication Geneva, 2010.
[8] Launch of Inmarsat swift broadband unmanned aerial vehicle service to provide operational capability boos, URL: https://www.inmarsat.com/press-release/launch-inmarsat-swiftbroadband-unmanned-aerial-vehicle-service-provide-operational-capability-boost/.
[9] I. Bekmezci, O. Sahingoz, S.Temel,: Flying Ad-Hoc Networks (FANETs): A Survey, Ad Hoc Networks 11(3) (2013) 1254–1270. doi: 10.1016/j.adhoc.2012.12.004.
[10] Y. Zhou, J. Li, L. Lamont, C. Rabbath, Modeling of packet dropout for UAV wireless communications, in: International Conference on Computing, Networking and Communications (ICNC), IEEE, Maui, HI, USA, 2012, pp. 677–682.
[11] Y. Zeng, J. Lyu, R.Zhang, Cellular-connected UAV: potentials, challenges, and promising technologies, Wireless Communications 26(1) (2019) pp. 120–127.
[12] T. Hong, K. Kang, K. Lim, J. Ahn, Network architecture for control and non-payload communication of UAV, in I 2016 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, Korea (South), 2016, pp. 762–764.
[13] Minimum Operational Performance Standards (MOPS) For Unmanned Aircraft Systems (UAS). Control and Non-Payload Communications Terrestrial Link Radio Systems, RTCA, 163-20/PMC-2034, 2020, URL: https://www.rtca.org/wp-content/uploads/2020/08/sc-228_tor_rev_10_approved_06-11-2020.pdf.
[14] R. Kerczewski, R. Griner, Control and Non-Payload Communications Links for Integrated Unmanned Aircraft Operations, in: 18th Ka and Broadband Conference, pp. 1-8. NASA, Ottawa, Canada, 2012.
[15] J. Griner, Unmanned aircraft systems (UAS) integration in the National Airspace System (NAS) project: UAS Control and Non-Payload Communication (CNPC) System Development and Testing, in: Integrated Communications, Navigation and Surveillance Conference (ICNS) Conference Proceedings, IEEE, Herndon, VA, USA, 2014, pp. 1–24. doi: 10.1109/ICNSurv.2014.6820072.
[16] S. I. Toufik, M. Baker, LTE The UMTS Long Term Evolution: From Theory to Practice. John Wiley & Sons Ltd, 2009.
[17] K. J. Matheou, et al. Analysis of at-Altitude LTE Power Spectra for Small Unmanned Aircraft System C2 Communications. In: Integrated Communications, Navigation and Surveillance Conference (ICNS), IEEE, Herndon, VA, USA, 2019, pp. 1–12. doi: 10.1109/ICNSURV.2019.8735287.
[18] R. A. Clothier, B. P.W illiams, N. L. Fulton, Structuring the safety case for unmanned aircraft system operations in non-segregated airspace, Safety Science 79 (1) (2015) 213–228.
[19] H. Menouar, I. Guvenc, K. Akkaya, A. S. Uluagac, A. Kadri, A. Tuncer, UAV-Enabled Intelligent Transportation Systems for the Smart City: Applications and Challenges, Communications Magazine 55(3) (2017) 22-28. doi: 10.1109/MCOM.2017.1600238CM.
[20] Y. Zeng, R. Zhang, T.J. Lim, Wireless communications with unmanned aerial vehicles: opportunities and challenges, Communications Magazine, 54(5) (2016) 36–42. doi: 10.1109/MCOM.2016.7470933.

[21] D. Rudinskas, Z. Goraj, J. Stankūnas, Security analysis of UAV radio communication system, Aviation 13 (2009) 116-121. doi: 10.3846/1648-7788.2009.13.116–121.
[22] A. Kim et al., Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. In: Infotech Aerospace Conference, pp. 2438. California, USA, 2012.
[23] N. Shashok, Analysis of vulnerabilities in modern unmanned aircraft systems,Review of the Air Force Academy 2(42) (2017) 17–26.
[24] X. Lin, et al. Mobile networks connected drones: field trials, simulations, and design insights. Vehicular Technology Magazine 14(3) (2019) 115-125. doi: 10.1109/MVT.2019.2917363.
[25] A. Abdallah, M. Z. Ali, J. Mišić, V. B. Mišić, Efficient Security Scheme for Disaster Surveillance UAV Communication Networks, Information 10(43) (2019) 1–22. doi: 10.3390/info10020043.
[26] C. Rani, H. Modares, R. Sriram, D. Mikulski, F. L. Lewis, Security of unmanned aerial vehicle systems against cyber-physical attacks, J. Defense Model. Simul.: Appl. Methodol. Technol. 13(3) (2015) 331–342.
[27] E. Basan, M. Lapina, N. Mudruk, E.Abramov, Intelligent Intrusion Detection System for a Group of UAVs, in: Advances in Swarm Intelligence. ICSI 2021. Lecture Notes in Computer Science, volume 12690. Springer, Cham., 2021. doi:10.1007/978-3-030-78811-7_22.
[28] E. Basan, A. Basan, A. Nekrasov, C. Fidge, J. Gamec, M. A. Gamcová, Self-Diagnosis Method for Detecting UAV Cyber Attacks Based on Analysis of Parameter Changes, Sensors 509 (2021) 1-17 https://doi.org/10.3390/s21020509.
[29] N. Proshkin, E. Basan, ,M. Lapina: Radio Frequency Method for Emulating Multiple UAVs, in: International Conference on Intelligent Environments (IE), 2021, pp. doi: 10.1109/IE51775.2021.9486599.