UAV COMMUNICATION PROTOCOLS AND QUALITY OF SERVICE IN 5G COMMUNICATION

Ovidiu PĂSCUȚOIU[*], Maria-Daniela TACHE (UNGUREANU)[**]

[*]"Henri Coandă" Air Force Academy, Brașov, Romania (ovidiu.pascutoiu@afahc.ro),
ORCID: 0009-0009-6918-0218
[**]"Politehnica" Bucharest National University of Science and Technology, Romania
(danielatache26@yahoo.com)
ORCID: 0009-0003-4588-8824

DOI: 10.19062/1842-9238.2024.22.1.1

Abstract: *This paper aims to provide an overview of common network protocols in UAV communications with a focus on security and vulnerabilities. In order to assess the common types of vulnerabilities, various elements must be taken into account such as mission purpose, communication type and protocol. The paper will walk through the main types of UAV protocols and make a brief analysis in terms of communication network security. It will also look on 5G communication requirements in terms of quality of service.*

Keywords: *Communication, Security, Networks, Vulnerabilities, Layer security, Data, UAV, Protocols*

1. INTRODUCTION

UAVs (Unmanned Aircraft Vehicles), commonly known as drones use specific protocols for communication with base stations. Over the last years, the increasing amount of UAVs missions both civilian and particularly military has raised the importance of UAV communication. More and more real-world applications use UAS (Unmanned Aircraft Systems) as a modus operandi; thus, UAVs as a part of UAS have become nearly indispensable to today's demanding complex operational activities such as air surveillance, intelligence, transportation just to name a few of them. In order to properly conduct communications between UAVs or inside an UAS (between UAV and base stations), communications must ensure an acceptable level of security. Bearing in mind that fulfilling an objective according to standards must be done within a certain level of security, this paper aims to have a quick look at most common UAV communication protocols from the security perspective. UAV-to-UAV and UAV-ground control station protocols will be presented in this paper.

2. LITERATURE REVIEW

As seen in the image above, aeronautical communication involves many types of communication whether we are talking about air to ground communication or air to air data transmission.

Some relevant paper regarding UAV communication include:

- [1] which describes UranusLink protocol from both architecture and security perspective;

- [2] presents some cyber-incidents identified within UAV communications from the military perspective;
- [3] describes different types of protocols used in drone swarm communications;
- [4] describe MAVLink protocol using ArduPilot Mega (APM) 2.8 is for conducting an experiment to demonstrate MAVLink features;
- In [5] the authors present the system architecture of the SUNNY project consisting of four UAVs communicating using DDS protocol;
- [6] make a security comparison between DDS, TLS and DTLS protocols outlining the key security components of DDS protocol.
- [7] present vulnerabilities on the MAVLink protocol.
- In [8], the authors propose a security-enhanced version of MAVLink called MAVSec which ensures confidentiality, availability, and integrity.
- [9] make an analysis of MAVLink protocol performance on ships.
- [10] make a comparison analysis between MAVLink, UAVCAN and UranusLink protocols in terms of architecture and security features.
- [11] present a survey through UAV communication vulnerabilities and types of attacks.
- [12] present D2GCS protocol security features.
- [13] experiment a DoS and hijack attack on UAV exploiting vulnerabilities on MAVLink protocol.
- [14] present a UAV 5G communication solution using a four antenna UAV coverage.
- [15] present a solution to encrypt MAVLink protocol using ChaCha20 as the encryption algorithm.
- [16] present a detailed analysis of UAV vulnerabilities.
- [17] propose a keystream cypher in order to enhance UAV communication through MAVLink protocol.

3. UAV COMMUNICATION PROTOCOLS

Most common protocols used in UAVs communication are:

- UranusLink;
- UAVCAN (Cyphal);
- MAVLink;
- DroneLink;
- DDS;

UranusLink as described in [1] is a communication protocol used for exchanging information between an UAV and a base station. The packet structure needed for transmitting data contains the following fields:

- Preamble;
- Sequence number;
- Message identification;
- Data Length;
- Data as such;
- Checksum;

UranusLink is a stateful protocol as it establishes connection between the UAV and the base station using a handshake mechanism. A secure version of this algorithm assumes that a symmetric algorithm such as AES will encrypt Message identification, Data, and checksum, leaving the other fields unencrypted in order to not alter the data

transmitted. Although challenges arise regarding the exchange of encryption keys, the algorithm itself can be considered secure as it provides a connection oriented, safe way to transmit information in order to be able to control an UAV from a base station.

UAVCAN or Cyphal [18] is a lightweight, open protocol for distributed communication among various types of intelligent vehicles including UAVs. The communication uses a client-server architecture and contains the following information needed for exchanging data:

- Payload;
- Data type ID;
- Client node ID;
- Server node ID;
- Transfer ID;

UAVCAN uses UDP as ISO/OSI transport protocol.

One of the most used protocols is Micro Air Vehicle Link Communication Protocol (MAVLink) which is a bidirectional communication protocol used for controlling UAVs from a ground control station. One ground control station can control up to 255 UAVs using MAVLink. The packet in version 2.0 contains 12 flags:

- Start;
- Payload length;
- Incompatibility flags;
- Compatibility flags;
- Packet sequence;
- Sender ID;
- Component ID;
- Message type;
- Data;
- Checksum with seed value A;
- Checksum with seed value B;
- Message authentication;

Although MAVLink does not support encryption by default, there are some papers describing various attempts in providing an alternative, secure version of MAVLink.

Data Distribution Service (DDS) protocol is an IoT protocol which operates between layer 4 (Transport) and layer 7 (Application) on the ISO/OSI architecture. It can work both on TCP and UDP. With UAVs, DDS can be used to establish communication between the base station and UAV. While DDS is not UAV specific, it can be used to ensure communication between intelligent devices. It supports AES for confidentiality and asymmetric encryption for key exchange and authenticity.

D2GCS represents a ground control station to UAV communication protocol which provides confidentiality, integrity, mutual authentication, and non-repudiation. It uses encryption algorithms such as ECDH for key exchange and digital certificates for encryption, authentication, and non-repudiation. Its best usage is military communication.

4. UAS COMMUNICATION SECURITY

In order to address modern-day challenges regarding UAV and UAS communications, security is a must. To better understand which of these protocols offers the best security, we will make a short comparison analysis of their characteristics.

	Connection type	**Geolocation**	**Open standard**	**Scalability**	**Overhead**	**Payload Integrity**	**Checksum**	**Security**	**Type of encryption (if supported)**
UranusLink	TCP	GPS	No	No	Small	Yes	Yes	Yes	AES
UAVCAN	UDP	GPS	Yes	No	Small	No	No	Limited	N/A
MAVLink	Mostly UDP	GPS	Yes	Yes	Large	No	Yes	No	N/A
D2GCS	TCP & UDP	GPS	Yes	Yes	Large	Yes	Yes	Yes	Symmetric and Asymmetric algorithms
DDS	TCP & UDP	GPS	Yes	Yes	Large	Yes	Yes	Yes	AES, RSA, ECDSA, DHE, ECDHE

5. QUALITY OF SERVICE IN 5G COMMUNICATION

We can say that 5G technology has reached a sufficiently high level of maturity, considering the variety of multimedia services and applications, as well as the capacity for their development, using dedicated slicing technology for media transport (audio, video, etc.), under the conditions of ensuring real-time data flow. From the perspective of Quality of Service (QoS), there is a set of essential parameters to which we can refer:

- Bandwidth: Ensures sufficient data flow so that the application operates without constraints in the production environment.
- Latency: Ensures minimal delay regarding real-time data flow.
- Jitter: Limits the delay of data packets circulating within the 5G network or within a slice.
- Loss: Restricts packet losses measured over a one-second interval

Considering the SMARTER study, conducted by 3GPP in 2015, whose purpose is to identify the characteristics and functionalities required for 5G technology, we can divide the technology's functionalities into three essential service categories:

- **eMBB** (Enhanced Mobile Broadband): Focused on providing high-speed data services, supporting applications like video streaming, augmented reality, and virtual reality.
- **mMTC** (Massive Machine-Type Communication): Geared towards connecting a massive number of IoT devices, sensors, and machines, enabling efficient communication at scale.
- **uRRLC** (Ultra-Reliable Low-Latency Communication): Designed for critical applications that demand extremely low latency and high reliability, such as industrial automation, remote surgery, and autonomous vehicles.

eMBB Services have the following characteristics:

- Real-time Video Streaming: eMBB services facilitate the transmission of real-time video streams, including alerts, using high-speed internet services.
- IoV (Internet of Vehicles): eMBB is also utilized within the IoV framework, aiming to interconnect autonomous vehicles.
- Transfer Rate Perspective: eMBB supports transfer speeds of 10 – 20 Gbps.
- Reliability for Vehicles: eMBB services are reliable even for vehicles traveling at speeds of up to 500 km/h.
- Aerospace and Unmanned Ground Vehicles: In the context of 5G, this technology plays a crucial role in data streaming while maintaining competitive Quality of Service (QoS).

- Technological Approach for Vehicle Communications: A multilayered stack built using Wi-Fi protocols enables communication between vehicles.

These protocols support various scenarios and can be adapted to vehicular traffic, as it follows:

- **GPSR-2p**: A position-based routing protocol that utilizes the transmission of coordinates in video format (Greedy Perimeter Stateless Routing).
- **VIRTUS**: A protocol that calculates the relative time between two vehicles to proactively estimate their future positions.
- **LIAITHON**: Considered a multipath or a module that identifies multiple routing paths based solely on the current location.

Considering that the network itself defines a perimeter zone, 5G can enable edge computing by allocating resources based on where they are needed. This improves data processing, reduces latency, and enhances response time for vehicles using 5G technology. [19]

7. CONCLUSIONS

Security is an important concern in ensuring UAVs communication throughout network protocols. As limited or no security would leave the door open to attacks such as man-in-the-middle, eavesdropping or identity spoofing, encryption and authentication would protect against these types of attacks. Still, it is still difficult to protect against flooding, DoS attacks jamming, therefore in addition to the security tools that come with the protocol, the physical security of both the UAV and the UAS, as a whole, is required.

REFERENCES

[1] V. K. &. P. Gabrlik, "UranusLink - Communication Protocol for UAV wish Small Overhead and Encryption Ability," *IFAC (International Federation of Automatic Control)*, pp. 474-479, 2015.

[2] K. H. &. K. Giles, "UAV Exploitation: A New Domain for Cyber Power," *2016 8th International Conference on Cyber Conflict*, pp. 205-221, 2016;

[3] C. A. S. &. M. Cardei, "Unmanned Aerial Vehicles Networking Protocols," *14th LACCEI International Multi-Conference for Engineering, Education, and Technology: Engineering Innovations for*, pp. 1-8, 2016;

[4] S. Atoev, K.-R. Kwon and S.-H. L. &. K.-S. Moon, "Data Analysis of the MAVLink Communication Protocol," *IEEE*, pp. 1-3, 2017;

[5] J. P. Ribeiro, H. Fontes, M. Lopes, H. Silva, R. Campos and J. M. A. &. E. Silva, "UAV Cooperative Perception based on DDS communications network," *IEEE*, pp. 1-8, 2017;

[6] M. Friesen, G. Karthikeyan, S. Heiss and L. W. &. H. Trsek, "A comparative evaluation of security mechanisms in DDS, TLS and DTLS," *Kommunikation und Bildverarbeitung in der Automation*, pp. 201-216, 2018;

[7] Y.-M. Kwon, J. Yu, B.-M. Cho and Y. E. &. K.-J. park, "Empirical Analysis of MAVLink Protocol Vulnerability for Attacking Unmanned Aerial Vehicles," *IEEE*, vol. 6, pp. 43203-43212, 2018;

[8] A. Allouch, O. Cheikhrouhou, A. Koubaa and M. K. &. T. Abbes, "MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems," *IEEE*, pp. 621-628, 2019;

[9] I. Nurmawati and A. A. &. I. Pratomo, "Evaluation of AIS and MAVLINK Protocol Performance," *International Seminar on Intelligent Technology and Its Applications (ISITIA)*, pp. 338-344, 2020;

[10] A. Khan, N. Z. Jhanjhi and S. N. B. &. A. Nayyar, "Emerging use of UAV's: secure communication protocol issues and challenges," *Drones in Smart-Cities: Security and performance*, pp. 37-55, 2020;

[11] N. A. Khan and S. N. B. a. N. Jhanjhi, "UAV's Applications, Architecture, Security Issues and Attack Scenarios: A Survey," *Intelligent Computing and Innovation on Data Science*, pp. 753-760, 2020;

[12] Y. Ko, J. Kim, D. G. Duguma, P. V. Astillo and I. Y. a. G. Pau, "Drone Secure Communication Protocol for Future Sensitive Applications in Military Zone," *Sensors*, pp. 1-25, 2021;

[13] H. Xu, H. Zhang, J. Sun, W. Xu, W. Wang and H. L. &. J. Zhang1, "Experimental Analysis of MAVLink Protocol Vulnerability on UAVs Security Experiment Platform," in *3rd International Conference on Industrial Artificial Intelligence (IAI)*, Shenyang, China, 2021;

[14] Y. Gao and P. W. &. J. Cao, "Intelligent UAV Based 5G Mobile Networks: A Cross Band Field Trial Results," *IEEE*, pp. 696-700, 2022;
[15] N. S. &. R. D. Daruwala, "Securing Unmanned Aerial Vehicles by Encrypting MAVLink Protocol," in *IBSSC*, Mumbay, India, 2022;
[16] H. J. Hadi, Y. Cao, K. U. Nisa and A. M. J. &. Q. Ni, "A comprehensive survey on security, privacy issues and emerging defence technologies for UAVs," *Journal of Network and Computer Applications*, pp. 1-26, 2023;
[17] N. A. S. &. R. D. Daruwala, "An approach to enhance the security of unmanned aerial vehicles (UAVs)," *The Journal of Supercomputing*, pp. 1-31, 2023;
[18] "uavcan.org," 2022. [Online]. Available: https://legacy.uavcan.org/l;
[19] A. B. M. B. F. M. M. S. e. a. C. Mannweiler, "5G Mobile Network Architecture for diverse services, use cases and applications in 5G and beyond," in *5G-Monarch*, Barcelona, 2018.