QUALITY OF SERVICE AND SECURITY OF AERONAUTICAL COMMUNICATION NETWORKS

Ovidiu PĂSCUȚOIU
"Henri Coandă"Air Force Academy, Brașov, Romania (ovidiu.pascutoiu@afahc.ro)
ORCID: 0009-0009-6918-0218

Maria-Daniela UNGUREANU
University "Politehnica" of Bucharest, Romania (danielatache26@yahoo.com)

DOI: 10.19062/1842-9238.2023.21.1.4

Abstract: *Aeronautical communication networks play a decisive role in the aviation industry, enabling real-time data exchange between various systems such ground stations, air traffic control and aircraft. Making sure that both requirements – high-quality-service and security – are met is mandatory to guarantee the efficiency, safety and reliability of aeronautical operations. This paper will go through a comprehensive inquiry of the quality of service and security of aeronautical communication and the relationship between them. The main focus of this paper is the security of aeronautical communications. The paper will examine the main types of aircraft communication types and will describe the cyber threats and the security measures applicable in order to mitigate the threats accordingly.*

Keywords: *communication, security, quality, service, encryption, digital, standard*

1. INTRODUCTION

Just like most industries, the aviation industry continues to embrace digitalization, therefore it is clear that aeronautical communications have become a critical concern.

There are many types of aeronautical communication networks, demonstrating how the digital era landscape has constantly evolved during the last 50 years.

Each type of aeronautical communication has its own particularities in terms of quality of service, performance and security.

This article will emphasize the quality of service and security of the main types of aeronautical communication, communication which is such a compulsory asset in order to properly carry out aviation operations.

The quality of service and aviation security are two different requirements; thus, they should be handled by means of different approaches, and with different objectives in mind. Of course, some QoS measure could alter security and vice versa, but this does not necessary mean that the two requirements are mutually exclusive.

Regardless of the type of communication considered (air to air communication/AAC or ground-based communication), security must be addressed and maintained properly in order to ensure the safety of aviation missions.

The paper is therefore composed of four parts:

- The types of aeronautical communications;
- Various QoS parameters for each type of communication;
- Specific cyber threats for these types of network communications;
- Security measures and solutions.

2. TYPES OF AERONAUTICAL COMMUNICATIONS

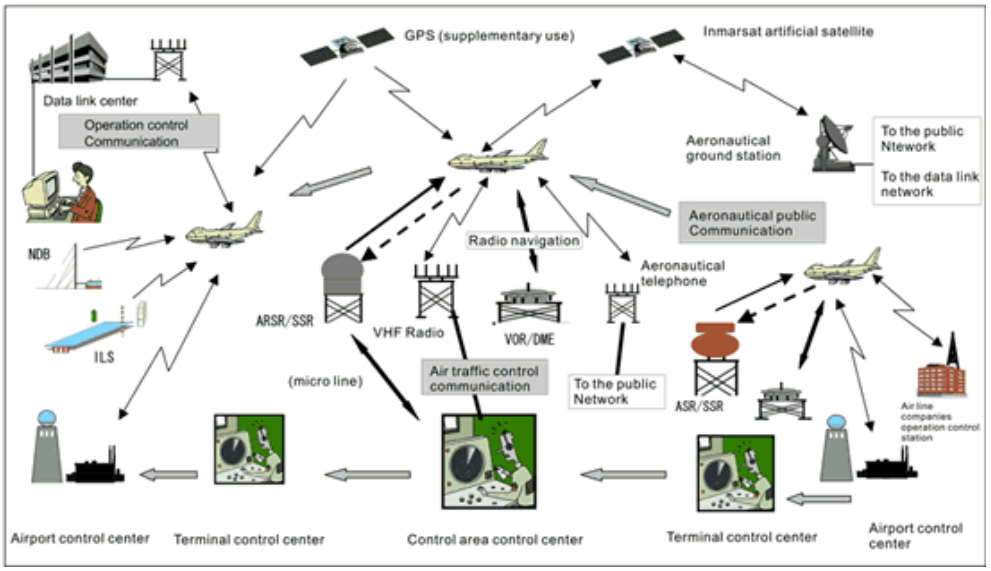

FIG. 1 Types of aeronautical communications

As shown 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.

The types of aeronautical communications can be classified as follows:

- **Analog** communications;
- **Digital** communications;
- **Radio Frequency Identification**;
- **Positioning** systems.

Analog communications can be divided into:

- Very High Frequency Voice Communication (**VHF**);
- High-Frequency Voice Communication (**HF**);
- Emergency Locator Transmitter (**ELT**);
- Navigational Aids.

Example of digital communication include:

- **VHF** Data Link;
- **VoIP** communication;
- **Satellite** communication;
- **Controller-Pilot** Data Link Communication system;
- Aircraft Communications Addressing and Reporting System (**ACARS**);
- Automatic Dependent Surveillance-Broadcast (**ADS-B**).

RFID systems can be divided into:

- **Active** RFID;
- **Semi-active** RFID;
- **Passive** (Battery-Assisted) RFID;
- Near Field Communication (**NFC**).

Positioning systems can be set up as:

- Global Navigation Satellite System (**GNSS**);
- Distance Measuring Equipment (**DME**);
- Tactical Air Navigation (**TACAN**);
- Microwave Landing System (**MLS**).

3. QUALITY OF SERVICE

In order to properly analyze the types of aeronautical communication, we will draw a comparison based on the criterion of the quality of service, as follows:

Table 1 – Quality of service parameters for different types of aircraft communication

Type of communication	Analog	Digital	RFID	Positioning systems
Latency	Variable	Low latency	Depending on read range and accuracy	Low latency
Reliability	Variable	Highly reliable	Reliable	Reliable
Availability	Line-of-sight based	Bandwidth dependent	High availability	Very high availability
Coverage	Ground-based transmitters	High coverage	Anti-collision algorithms based	Very high coverage
Interference	Susceptible to interference	Low interference	Susceptible to interference	Very low interference
Audio quality	Noise reduction	High quality	N/A	N/A
Integration with other systems	No	Interoperability with other communication systems	Allow integration but not a main concern	Yes
Security	Low security / No security	High concern	Vital	High concern
Frequency management	Important	Critical	Essential	N/A

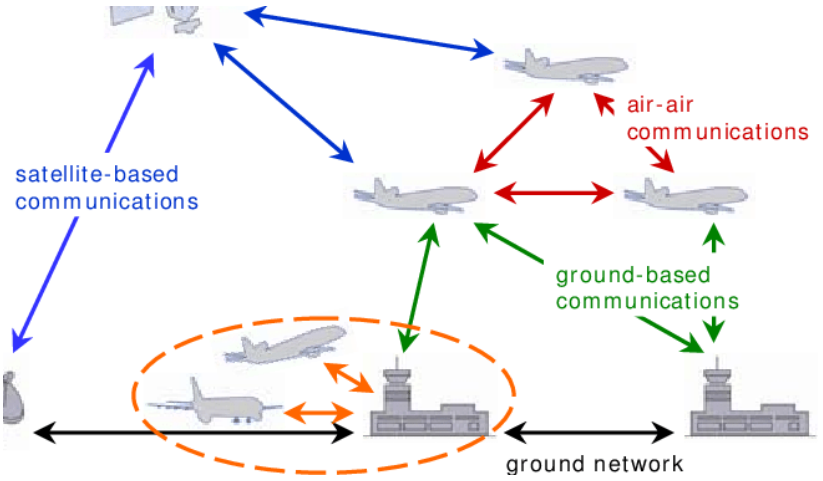

FIG. 2 Aeronautical communication

4. CYBER-THREAT LANDSCAPE

There are many challenges regarding aviation security. Some examples include but not limited to:

- Signal interference;
- Limited bandwidth;
- Unsecure channels;
- Lack of security awareness.

These vulnerabilities can lead to potential damage depending on the attack vector and the surface area.

Table 2 – Main cyber threats-attack vector-damage in aviation communications

Cyber threat	Attack vector	Potential damage
Unauthorized access	Communication systems	Disruptions
Data breaches	Insider threats or collected data	Critical information compromised
Malware	Communication networks	Data integrity compromised
DDoS attacks	Any communication traffic	Inaccessible or degrading communication with flood or traffic
GPS spoofing or jamming	GPS signals	Manipulated aircraft navigation, jammed or blocked GPS signals
Social Engineering	Phishing email	Exposure of systems to cyber threats

(F. Shaikh, 2019) presents a matrix of security threats classified by cyber threat type:

Table 3 *(F. Shaikh, 2019)* security matrix of E-enabled systems

Denial of Service (DoS) attacks	Communication Jamming attacks	Spoofing	Man-in-the-Middle & Eavesdropping attacks	In-flight cyber attacks	IT vulnerabilities
DoS on airport communication infrastructure	Attacks on GPS-based navigation aids	Lack of authentication in CPLDC	Critical information leakage	DoS jamming attacks	Lack of regulations in COTS hardware/soft ware
ATM DoS	RF transmitters interference with GPS signal reception	Message manipulation	Lack of integrity checking	Wideband jamming attacks	Traditionality of security mechanisms in modern aircrafts
Wormhole attacks	Direct interference of GPS signals	Easy impersonation	Lack of encrypted messages for ADS-B transmission	Cross-layer jamming attacks	Traditionality of IP-based networking interconnectio n in ground-based aircrafts
	Intentional interference of GPS signals	False message injection	Eavesdropping on wireless channel	Reactive jamming attacks	Lack of protection of air network traffic from unauthorized access & information leakage
	Direct jamming of GPS signals	Delay injection	Ground-based Man-in-the-Middle attacks		
	Jamming attacks on radio altimeters	Access of ICAO values via Internet	Disrupt/alter control signals		
		Generation of misleading ATC location profiles			
		Spoofing GPS readings of longitude and latitude			
		Generation & pseudo-matching real aircraft flight behaviors			

Nowadays, technologies such as Software-Defined Networks, Internet of Things (IoT), 5G communications are susceptible to various cyber threats, most of them are denial-of-service, spoofing and data leakage.

In the past three years, there have been some powerful attacks which led to global-scope consequences. The most important ones are presented in the table below.

Table 4 – Cyber-attacks in aviation

Date	Airline / Organization / Country	Type of attack	Consequences
25 May 2022	SpiceJet / India	Ransomware	**Several hours** disruption of services
April 2022	SunWing Airlines / Canada	DDoS	**4 days** extensive flight delays
March 2022	Russian CAA / Russia	APT	**65 TB** of data deleted
March 2021	SITA / Singapore Airlines / Air India Singapore, India	Data breach	**580.000** flying members data compromised (Singapore) **4.5 million** passenger data stolen
2020	VT San Antoni Aerospace, USA	Ransomware	**1 TB** data stolen, encrypted networks, 3-day system recovery
2020	easyJet, UK	Social Engineering	**2208** customers' information disclosed

5. SECURITY MECHANISMS

Depending on the cyber threat type and the attack surface, there are various security mechanisms which can be implemented.

Table 5 – Security mechanisms

Cyber threat	Attack vector	Potential damage
Unauthorized access	Disruptions	Authentication mechanisms, SRTP
Data breaches	Critical information compromised	PKI infrastructure, Radio channel integrity
Malware	Data integrity compromised	Air Traffic management security, PKI infrastructure
DDoS attacks	Inaccessible or degrading communication with flood of traffic	Radio channel integrity Traffic data control mechanisms
GPS spoofing or jamming	Manipulated aircraft navigation, jammed or blocked GPS signals	Signal monitoring and anomaly detection
Social Engineering	Exposure of systems to cyber threats	Personnel awareness

These security mechanisms must be adopted and implemented in accordance with the newer technologies and must be updated and replaced, if necessary, as emerging technologies such as artificial intelligence and quantum computers thrive.

CONCLUSIONS

It is obvious that ensuring the quality of service and security of aeronautical communications is not an easy task, but a mandatory one. Features like reliability, latency, and bandwidth or quality metrics are essential characteristics to take into consideration when designing proper aeronautical communication architecture.

If the quality of service can be ensured at a proper level by design, with security, is a more complicated issue. Security is not something that can be maintained at a very high level for a long period of time. More and more sophisticated types of attacks emerge, making it harder and harder for engineers to mitigate attacks and protect the aircraft communication infrastructure.

In conclusion, this paper emphasizes the critical importance of simultaneously addressing QoS and security in aeronautical communication networks. Achieving a balance for the two requirements is indispensable for the safe, efficient and dependable operations of aircraft systems in an increasingly security-threaten, interconnected digital environment.

REFERENCES

[1] F. Shaikh, M. Rahouti, N. Ghani, K. Xiong, E. Bou-Harb, J. Haque – "*A Review of Recent Advances and Security Challenges in Emerging E-Enabled Aircraft Systems"*, IEEE, 2019;

[2] H. Duchamp, I. Bayram, R. Korhani – "*Cyber-security, a new challenge for the aviation and automotive industries*", J. Strategic Threat Intell, 2016

[3] R. K. Rakaselaran, E. Frew – "*Cyber security challenges for networked aircraft*", IEEE, 2017

[4] M. Strohmeier, M. Shafer, R. Pinheiro, V. Lenders, I. Martinovic – "*On perception and reality in wireless air traffic communication security*", Trans. Intell. Transp. Syst, 2017