RADemics

Secure Drone Communication Using Cloud-Based Encryption and Cybersecurity Frameworks

Amit Joshi, S. Muthurajan
Riga Nordic University and BA School of Business and Finance, , Academy of Maritime Education and Training (AMET), Deemed to be University

Secure Drone Communication Using Cloud-Based Encryption and Cybersecurity Frameworks

[1]Amit Joshi, Lecturer and Researcher, Department of Computer Technologies and Natural Sciences, Riga Nordic University and BA School of Business and Finance, Riga, Latvia. Amit.joshi00008@gmail.com

[2]S. Muthurajan, Assistant Professor, Department of Marine Engineering, Academy of Maritime Education and Training (AMET), Deemed to be University, ECR, Chennai, Tamil Nadu, India. smuthuraajan@gmail.com

Abstract

The increasing adoption of unmanned aerial vehicles (UAVs) across various industries has highlighted the critical need for securing drone communication systems. As drones become more autonomous and integral to mission-critical operations, safeguarding their communication networks from evolving cyber threats is paramount. This chapter explores the intersection of cloud-based encryption, cybersecurity frameworks, and AI-driven technologies to enhance the security of drone communications. It delves into the role of secure key distribution methods, advanced encryption techniques, and real-time threat detection systems in ensuring data integrity, confidentiality, and operational reliability. The integration of edge computing is also discussed, emphasizing its impact on real-time threat mitigation by reducing latency and enabling autonomous responses to security breaches. Furthermore, the chapter examines the challenges associated with scalable security solutions in large drone networks and highlights emerging technologies such as blockchain and machine learning as potential solutions for strengthening UAV security. This research aims to provide a comprehensive framework for securing drone communication systems, ensuring that UAVs can operate safely and effectively in increasingly complex environments.

Keywords: Drone Communication, Cybersecurity, Cloud-Based Encryption, AI-Driven Security, Edge Computing, Key Distribution.

Introduction

The rise of unmanned aerial vehicles (UAVs) has revolutionized multiple industries, enabling more efficient, cost-effective, and scalable solutions across sectors like logistics, surveillance, defense, and agriculture [1]. Drones, equipped with advanced sensors, cameras, and communication systems, have quickly become an essential tool for carrying out tasks that were once time-consuming, hazardous, or impossible for humans to perform [2]. As drones are integrated into more mission-critical operations, securing their communication networks becomes an urgent necessity [3]. Drone communication systems are inherently vulnerable to various cyber threats due to their reliance on wireless networks, which exposes them to risks such as data

interception, unauthorized access, and signal jamming. Therefore, robust security measures are essential to ensure that UAVs can operate reliably and securely, without compromising mission integrity [4].

One of the primary challenges in securing drone communication systems is the need to protect sensitive data while maintaining real-time communication between drones and ground control stations [5]. Traditional security methods often fail to meet the requirements of modern UAV networks, which demand low-latency, high-bandwidth communication in highly dynamic environments [6]. Cloud-based encryption techniques offer a promising solution by offloading complex encryption tasks from drones to cloud platforms, providing the computational power necessary to secure data without overburdening the drone's limited onboard resources [7]. These encryption methods ensure that the data exchanged between drones and control stations remains confidential and intact, even in the presence of external threats [8].

In addition to cloud-based encryption, the adoption of comprehensive cybersecurity frameworks is critical for ensuring the security of drone systems [9]. Frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 provide guidelines for implementing security controls, risk management strategies, and incident response protocols within UAV networks [10]. These frameworks help define best practices for securing data transmission, preventing unauthorized access, and addressing vulnerabilities within the drone's software and hardware [11]. By adhering to these established cybersecurity standards, UAV operators can build more resilient systems capable of withstanding a wide range of cyber threats while ensuring compliance with international security requirements [12].

Edge computing is another emerging technology that significantly enhances the security of drone communication networks. Edge computing involves processing data locally on the drone or at a nearby network node, rather than relying on distant cloud servers for data analysis [13]. This decentralization reduces latency and minimizes the risks associated with transmitting sensitive data over long distances. In the context of cybersecurity, edge computing enables drones to detect and respond to threats in real time, without waiting for data to be sent to a centralized server [14]. For instance, a drone equipped with edge computing capabilities can autonomously identify signs of signal interference or unauthorized access and take immediate countermeasures, such as changing communication frequencies or activating enhanced encryption protocols, to mitigate the threat [15].