**Fast, Reliable, and Secure Drone Communication: A Comprehensive Survey**

**APA:** Hassija, V., Chamola, V., Agrawal, A., Goyal, A., Luong, N. C., Niyato, D., ... & Guizani, M. (2021). Fast, reliable, and secure drone communication: A comprehensive survey*. IEEE Communications Surveys & Tutorials*, 23(4), 2802-2832.

1. Summary of Part III.A: *Drone Communication Architecture Using Blockchain*

This article explores the use of blockchain technology to enhance the security of drone communications, given the rapid increase in drone usage and associated data. Blockchain provides a distributed, tamper-proof system that protects drone data from unauthorized access. It ensures that transactions between drones and users are secure, cost-effective, and privacy-preserving. Smart contracts and various types of blockchain networks can be tailored to meet the specific needs of drone applications. Overall, blockchain is presented as a promising solution to make drone communication more secure, reliable, and efficient.

1. Summary of Part III.B: *Drone Communication Architecture Using SDN*

This article discusses the application of Software-Defined Networking (SDN) in drone communication architectures, where SDN allows for centralized control of the network through software applications. In an SDN-based drone network, each drone acts as an individual switch, and the network's control and data planes are decoupled, offering flexibility in design. SDN enables direct programmability and reliable management, making it suitable for real-time applications like video streaming. The centralized control of SDN enhances security by closely monitoring data traffic and mitigating vulnerabilities inherent in resource-constrained drones. The article suggests that SDN can significantly improve the security and efficiency of drone communication networks, with further models discussed in a subsequent section.

1. Summary of Part III.C: *Drone Communication Architecture Using Machine-Learning*

This section explains how machine learning (ML) can enhance the security of drone communication by enabling systems to learn and improve automatically from past experiences without explicit programming. ML algorithms require large amounts of training data to make accurate predictions and can be categorized into supervised and unsupervised learning. Various ML techniques, such as CNN, SVM, and LSTM, can be applied to secure drone communication by detecting faults, classifying data packets, and preventing attacks like DoS and man-in-the-middle. The adaptability and accuracy of ML algorithms, which improve with experience, make them ideal for securing drone networks. The section also highlights that further details on ML techniques for securing drone communication are provided later in the article.

1. Summary of Part III.D: *Drone Communication Architecture Using Fog Computing*

This section introduces fog computing, a concept developed by CISCO in 2014 as an extension, rather than a replacement, of cloud computing. Fog computing serves as an intermediary layer between edge devices and the cloud, offering a more cost-effective, time-efficient, and secure alternative to deploying cloud servers. By processing and storing data closer to the end devices, fog computing reduces latency, minimizes the load on cloud servers, and enhances data security through decentralization. These benefits make fog computing particularly advantageous for improving the quality of service and security in drone communication. The section also notes that further details on fog-based models for securing drone communication are discussed later in the article.