Chapter 8
Decentralized Security for Smart Drone Surveillance System Architecture and Communication

Isha Malhotra
https://orcid.org/0000-0003-3027-6158
Dronacharya College of Engineering, India

Kumari Anshu
https://orcid.org/0009-0000-8959-4252
Dronacharya College of Engineering, India

Sushant Jha
Dronacharya College of Engineering, India

ABSTRACT

The integration of decentralized security mechanisms into smart drone surveillance systems marks a transformative advancement in the field of unmanned aerial monitoring. Traditional centralized architectures are often vulnerable to single points of failure, data breaches and latency issues specifically in case of operation in hostile or remote environments. By leveraging blockchain technology, drone networks can establish a tamper-proof, distributed ledger that ensures the integrity and authenticity of surveillance data in real time. Internet of Drones is a decentralized network linking drones access to controlled airspace, providing high adaptability to complex scenarios and services to various drone applications such as package delivery, traffic surveillance and rescue including navigation services. One of the potential methods to enhance user privacy, data security and authentication, especially in peer-to-peer UAV networks is blockchain technology, which has now been gained prominence.

DOI: 10.4018/979-8-3373-4277-1.ch008

1 INTRODUCTION

Unmanned aerial vehicles (UAVs) are high-end cyber-physical systems (CPSs) for numerous data collection and monitoring tasks. Drones were initially designed as a simple device nevertheless have grown in complexity as defined missions have become more complex. The diversity of drones is a primary factor in defining their operational capabilities which are determined by their size, power and application conditions. UAVs are classified into two parts including HTA (Heavier than Air) and LTA (Lighter than Air) (Ozoroski, Nickol & Guynn(2015)). Specifically, the use of UAVs in disaster has the subsequent benefits such as they reduce the time required to locate victims and the time required for subsequent intervention by searching a large area in a short period of time, in addition to providing critical information to rescuers about the route that needs to be taken during search and rescue operations. Additionally, drones are capable of searching for alive victims buried beneath rubble using sensors such as noise sensing, binary sensing, vibration and heat sensing (Herrera Velasco, 2024). The limitations of existing robotic solutions, often constrained by their reliance on single locomotion modalities, become particularly apparent when navigating the diverse and challenging environments encountered in disaster zones. Until recently, drones were operated individually. However, recent technological accomplishments allow a high number of drones to interconnect and accomplish complex missions coordinately, aiming for the efficient management of their airspace (Luo, 2025)- (Kopardekars,2015). Such approaches have led to the rise of the Internet of Drones (IoD) ecosystem (Mandloi, Arya, & Verma, 2024). The IoD is considered to be a part of the Internet of Things (IoT), equipped with interconnected physical devices and Internet-connected sensors. As a typical network architecture, it enables communications between UAVs and devices on the ground in a coordinated manner, allowing drones to have flight control and providing navigation services such as the internal transmission and exchange of data, with integrated mobility, portability and automation.

Advanced airborne platforms known as “smart drone surveillance systems” integrate data analysis, mobility and sensing to monitor areas on their own. Decentralized security is crucial in this context because, instead of depending on a single command center, security tasks like data validation and authentication are distributed throughout the network via blockchain technology. As a node in the network, every UAV keeps an encrypted, impenetrable record of all communications and updates. The architecture encompasses both the digital backbone, which consists of fault-tolerant technology, distributed processing and onboard intelligence, as well as the physical components, such as our walking-flying hybrid drones. Communication's function is to connect all UAVs over peer-to-peer (Ameur, Oubbati, Lakas, Rachedi, & Yagoubi, n.d.), encrypted channels, frequently via blockchain protocols. This eliminates the need for a ground station or continuous internet access, enabling them to exchange real-time data, plan motions and work together intelligently. These ideas come together to create a safe, flexible and self-sufficient surveillance system in which every drone functions as more than just a sensor but as an intelligent, dependable team member.

Smart drones with decentralized security and autonomous communication architectures are becoming indispensable for real-time, adaptive monitoring in a time when intelligent aerial technologies are revolutionizing modern surveillance. Decentralized drone networks disperse security procedures and decision-making among all individual units, in contrast to traditional systems that depend on central control. As a result, they are more scalable, resilient and quick to react in situations involving sensitive data or high risk. New developments in drone technology, such as hybrid drones that can fly and walk, offer even more versatility in complex terrains and urban spaces.