Chapter 12
Blockchain-Integrated Security Models for Data Integrity in Drone-Based Surveillance Using Wireless Sensor Networks

Spinder Kaur
Chandigarh University, Mohali, India

Rohit Bajaj
Chandigarh University, Mohali, India

Manoj Kumar Pandey
https://orcid.org/0000-0002-2880-4997
Chandigarh University, Mohali, India

Celestine Iwendi
https://orcid.org/0000-0003-4350-3911
University of Bolton, UK

Tien Anh Tran
University of Malta, Msida, Malta

ABSTRACT

The integration of unmanned aerial vehicles (UAVs), or drones, with Wireless Sensor Networks (WSNs) has been a successful solution to improve real-time monitoring in military operations, mainly in the border area. WSNs and UAVs, or drones, have been utilized to improve real-time monitoring in military operations, mainly in border areas. The model utilizes advanced defence grade sensors, such as LiDAR for accurate object detection and topography mapping and magnetometers to detect anomalies in the magnetic field that would indicate hidden metallic threats or buried activities. By adding blockchain technology to the communication infrastructure, the system provides tamper-proof, transparent, and

DOI: 10.4018/979-8-3373-4277-1.ch012

decentralized storage of sensor data and shields against unauthorized access and manipulation. This chapter shows some simulation results and threat analysis demonstrates the immunity of the model against cyber-attacks and performance in ensuring trust in defence surveillance operations.

1. INTRODUCTION

The integration of blockchain and Wireless Sensor Networks (WSNs) in drone-based surveillance systems offers a viable solution to data integrity, security, and trust in mission-critical applications such as smart city surveillance, disaster relief and military surveillance (Hentati & Fourati, 2020; Mohsan et al., 2023). A security model based on blockchain is described in this chapter to counter the threats of drone-based WSNs, such as data tampering, unauthorized access and communication inefficiencies. The proposed model indicated tamper-evident data storage and secure communication that leverage the decentralised, immutable and cryptographic characteristics of blockchain. The method is a hybrid blockchain system that uses a lightweight consensus and edge computing for the best performance in resource-limited drone environments, allowing it to operate at its full potential (Wadhwa et al., 2025). The simulation findings show that there is an improved data integrity (98% verification rate) and encryption efficiency (0.5ms per packet), thus asserting the capability of the model (Nguyen et al., 2021). The given literature addresses the issues of scalability, interoperability and energy efficiency (Nguyen et al., 2024). The rapid development of Unmanned Aerial Vehicles (UAVs), or drones, has made the surveillance and monitoring processes and their utilization real-time and data collection in a range of settings. With WSNs drones create a solid platform for applications such as smart city surveillance, precision agriculture, environmental monitoring, border monitoring, and search and rescue (Nguyen et al., 2021). In intelligent cities, sensor-laden drones patrol traffic, air quality, and infrastructure conditions to feed life-saving data to city infrastructure planning and public safety. For agriculture, precision crop and soil health monitoring is made possible by them, optimizing resource utilization and crop yield. In search and rescue operations, thermal and visual sensor-laden drones increase situational awareness in emergencies, optimizing response time (Nguyen et al., 2021). The open wireless environment of WSN and the limited resource of drones, however, make the systems extremely susceptible to a wide range of security attacks like man-in-the-middle attacks and data exposure, eavesdropping, spoofing, and data tampering (Hentati & Fourati, 2020; Mohsan et al., 2023). Attacks are of critical significance in time-critical missions, where compromised or altered data result in incorrect decision making, the effects of which may be damaging to or loss of life or infrastructure.

WSNs and drones as a combination pose a unique challenge because such a system by nature is resource-limited and dynamic. Drones themselves are also generally resource-limited with limited processing capabilities, limited battery life, and intermittent connectivity and thus security mechanisms like heavyweight encryption or centralized authentication are not possible (Pawar et al., 2025). In addition, mobility and decentralized nature of drone networks increase risks such as spoofing where attackers pretend to be legitimate nodes or eavesdropping, where sensitive information is intercepted while in transit. Integrity, confidentiality, and authenticity of the information become of particularly grave concern in such a system because even slight manipulation of information would be disastrous in uses such as military reconnaissance or emergency response (Nguyen et al., 2021).