

Research on security issues and Blockchain applications in wireless sensor networks

Somneuk Vongthavihoung

Abstract: This study investigates critical security vulnerabilities in Wireless Sensor Networks (WSNs) and proposes a Blockchain-based framework to address them. WSNs, characterized by resource-constrained nodes and decentralized architectures, are inherently susceptible to attacks such as data tampering, node compromise, and denial of service. Traditional centralized security solutions often introduce single points of failure and scalability bottlenecks. This research explores the integration of Blockchain technology to enhance data integrity, authentication, and trust management within WSNs. A lightweight consensus mechanism is designed to accommodate the limited computational and energy resources of sensor nodes. The proposed model ensures immutable data logging and decentralized access control, mitigating risks of unauthorized data manipulation. Performance evaluation through simulation demonstrates that the Blockchain-enhanced WSN achieves improved resilience against common attacks while maintaining acceptable latency and energy consumption levels. The findings confirm that Blockchain offers a viable, decentralized security layer for WSNs, particularly in applications requiring high data fidelity and auditability, such as environmental monitoring and smart infrastructure.

Keywords: Blockchain, security, wireless sensor networks, applications