Abstract

Wireless Sensor Networks (WSNs) are increasingly being deployed in a wide range of applications, including environmental monitoring, smart healthcare, industrial automation, and military surveillance. Despite their versatility, WSNs are inherently prone to security threats due to characteristics such as constrained energy resources, open communication channels, and often remote or unattended deployments. These vulnerabilities are especially critical at the routing layer, where attacks such as Sybil, wormhole, blackhole, and selective forwarding can significantly disrupt network operations. To address these challenges, secure routing protocols have been proposed to ensure data integrity, confidentiality, and reliable packet delivery. This paper presents a systematic literature review of secure routing protocols in WSNs, conducted following the PRISMA 2020 guidelines. The review is guided by three central research questions: (1) What are the main attacks in WSNs and the methods/techniques used to mitigate these attacks? (2) What secure routing protocols have been developed for Wireless Sensor Networks, and what are their respective strengths, weaknesses, and areas of application? (3) What strategies that may influence the future design of secure routing protocols in WSNs? A total of 40 peer reviewed publications from 2019 to 2025 were selected from reputable databases including IEEE Xplore, SpringerLink, ScienceDirect, MDPI, Wiley Online Library, and the ACM Digital Library. The analysis reveals a range of attack mitigation strategies and secure routing protocols such as SEARP, ITEERP, ESR, SeRINS, and IASR. Each protocol offers different trade-offs in terms of security robustness, energy consumption, scalability, and adaptability. Furthermore, trends such as artificial intelligence, edge computing, and lightweight cryptographic methods are identified as key drivers for future protocol development. This review looks at current research and outlines areas for future exploration in secure WSN routing.