

Trust management framework for securing software-defined wireless sensor networks

International Conference on Electrical, Computer and Energy Technologies (ICECET), 16-17 November 2023, Cape Town, South Africa

Abu-Mahfouz, Adnan MI
Council for Scientific and Industrial Research (CSIR)
Meiring Naude Drive, Pretoria, 0184
Email: AAbuMahfouz@csir.co.za

The growing application of wireless sensor networks (WSN) has unveiled several opportunities for innovative services and data-driven applications. However, the WSN's inherent vulnerabilities and challenges have raised considerable concerns about data security and integrity despite inventions like software-defined networking. Therefore, this paper proposes a comprehensive trust management framework (TMF) to address Software-defined WSN (SDWSN) security challenges. The proposed TMF capitalizes on the dynamic and flexible nature of the SDWSN to establish trust relationships, both between sensors (S2S) and between controllers and sensors (C2S). Leveraging behavioural analysis, the framework evaluates packet forwarding ability for S2S trust based on reputation, while employing a recommendation-based scheme based on anomalous traffic detection for C2S trust. By analyzing the network traffic, the TMF enhances the trustworthiness assessment and decision-making process. The framework allows the efficient and reliable identification of malicious nodes, unauthorized access, and data tempering within the network. While the proposed TMF is currently in the development stage and awaits implementation and evaluation, its potential impact on improving network security in the SDWSNs is promising.