Chapter 10
Intrusion Detection Framework for Industrial Wireless Sensor Networks in Smart Manufacturing

M.Nirmal Kumar
https://orcid.org/0009-0001-1530-2680
Bharath Institute of Higher Education and Research, India

T. Vijayan
https://orcid.org/0000-0001-9383-5960
Bharath Institute of Higher Education and Research, India

B. Karthik
Bharath Institute of Higher Education and Research, India

ABSTRACT

IWSNs are necessary for smart manufacturing because they allow the continuous monitoring and control of resources. However, their susceptibility to cyber threats requires enhancing efficient and effective IDS systems. The proposed work introduces a newly developed approach based on ML and DL techniques to achieve efficient intrusion detection in IWSNs. The framework offers feature extraction using higher-order features and dominant Eigenspace to enhance the detection accuracy while maintaining enhanced computational time and selecting adaptive thresholds. The performance analysis against benchmark datasets shows a high level of effectiveness with a detection accuracy of 99.2%, precision of 97.9%, recall ratio of 98.3%, and F1 Score of 98.1%. Moreover, the experimental results show a decreased detection delay and improved resource efficiency, making the system ideal for real-time ap-

DOI: 10.4018/979-8-3373-4672-4.ch010

plications in smart manufacturing systems. However, the proposed framework is superior to the previous solutions in terms of accuracy and required time.

INTRODUCTION

IWSNs are a key infrastructural enabler in the current smart manufacturing paradigm because they facilitate real-time monitoring and communication of the production processes. IWSNs have become especially relevant in Industry 4.0 initiatives to improve processes and performance and increase the efficiency of tangible assets with connected devices. It enables smooth integration of inter- and intra-organizational data flow, promoting advanced intelligent automation (Yang et al., 2024). However, these have brought significant risks of cyberattacks such as DoS attacks, data manipulation, and unauthorized access, compromising the manufacturing systems and their data (Zhibin, 2021). These issues called for strong intrusion detection to enhance the reliability of IWSNs while in operation. While IDS solutions for IWSNs have recently attracted the attention of researchers, the existing ones experience some essential drawbacks (Islam et al., 2024). Classic rule-based methodologies relying on rigid process protocols are not particularly versatile in rapidly evolving industrial systems. Despite these advantages, typical machine learning (ML) methods appear to struggle with the problem of imbalanced datasets, thus leading to high false positives and weak generalization. For instance, it involves minimal feature extraction techniques and does not consider higher-order dependencies of the sensor data, resulting in a low detection rate (Mishra et al., 2024). Furthermore, computational models, including deep learning DL methods that include CNNs and RNNs, have high computational costs, limiting their execution on constrained devices (Sundararajan et al., 2023).

Furthermore, most existing frameworks do not possess the censoring mechanism for real-time monitoring. They thus cannot be used to address dynamic threat situations prevalent in industrial environments (Yuan et al., 2023). These constraints underscore the importance of a new approach for scale, precision, time complexity, and dynamic system behavior. The rationale for this work emerged from the enormous demand for defending IWSNs facing emerging cyber threats without compromising the functionality of smart manufacturing systems. Contemporary trends clearly show that opponents enhanced their activities in the cyber environment, increasing the attractiveness of attacking industrial systems with the help of their integration and wireless connections (Harendharan and Rahmouni, 2023).

Mitigating these vulnerabilities is crucial to avoid increased financial risks, production loss, and data breaches. In addition, utilizing more complex technologies like ML and DL is highly promising for improving the accuracy of the intrusion