Chapter 12
Real-Time Threat Detection on Machine Learning Approaches in Wireless Sensor Network Security

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

Wireless Sensor Networks (WSNs) play a vital role in applications like environmental monitoring and military operations but face significant security challenges such as Denial of Service (DoS), Sybil, and sinkhole attacks. Traditional security mechanisms are ineffective due to their reliance on static rules, high false positive rates, and limited scalability. This chapter introduces a machine learning (ML)-based real-time threat detection system using Decision Trees (DT), Support Vector Machines (SVM), and Neural Networks (NN) to identify network anomalies dynamically. The system preprocesses real-time sensor data, extracts relevant features, and continuously retrains models to detect both known and novel attacks with high accuracy.

DOI: 10.4018/979-8-3373-4672-4.ch012

Compared to existing systems, the proposed approach demonstrates superior performance, achieving 95.1% accuracy versus 85.7% and 82.3% for previous models. It enhances detection accuracy (97.5%) and true positive rate (95.8%), making it more reliable for intrusion detection.

INTRODUCTION

WSNs have been employed in many of today's most prevalent applications, including environmental monitoring, health care, industrial automation, smart cities, military monitoring, and agriculture. These networks comprise several low-power sensor nodes communicating wirelessly to gather and transmit data across great distances. The primary advantage of WSNs is the ability to gather real-time information on various environmental and operational factors in remote geographical areas that are normally difficult or impossible to reach (Ahmad et al., 2022). Nonetheless, the characteristics of WSNs with limited resources make them vulnerable to cyber threats that can jeopardize their integrity, access, and confidentiality. WSNs differ from traditional networks in that these generally operate in hostile environments where adversaries can exploit physical and software restrictions such as sensor node energy, processing power, and communication capabilities. This presents a significant problem for network security, as traditional security measures often fail to provide appropriate protection in these highly resource-constrained and unpredictable contexts. Because of the prevalence of severe if-WSNs in important applications, the security of WSNs has been one of the most extensively researched fields of study in recent years. DoS, data modification, unauthorized data access, data integrity loss, and physical damage to nodes or infrastructure could all be attributed to WSN assaults. Traditional security solutions such as encryption, authentication, and intrusion detection systems (IDS) cannot counter the threats to WSNs. Traditional IDS uses signature-based detection, which only works against known threats. Such strategies are often slow and unable to detect novel or changing assault patterns (Ifzarne et al., 2021).

Furthermore, the high false positive rates exacerbate the problem by wasting resources and impairing network performance. More advanced and adaptive security systems are urgently needed to identify and successfully block known and unexpected assaults. The chapter is inspired by the growing demand for new and more advanced threat detection systems that can operate in resource-constrained WSN environments(Jiang et al., 2020). Given the expanding volume and complexity of WSNs, systems that can handle novel and developing security threats will be required. ML)is a promising solution to overcoming these issues since it automatically learns patterns from data and can use learned patterns to anticipate