IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

Robust Intrusion Detection System for Military Wireless Sensor Networks Applications

Sumedh Dhengre[1], Upeksha Kohak[2], Rajnandini Patil[3], Sagar Swami[4], Ayush Suryavanshi[5]
Guide, Department of Computer Engineering[1]
Students, Department of Computer Engineering[2,3,4,5]
AISSMS COE, Pune, Maharashtra

Abstract: *Wireless Sensor Networks (WSNs) play a crucial role in modern military communication and surveillance but are increasingly vulnerable to cyberattacks due to their distributed and resource-constrained nature. Traditional security measures such as encryption and firewalls are insufficient for real-time threat detection in these environments. This research aims to design a lightweight Intrusion Detection System (IDS) using machine learning algorithms—Decision Tree, Random Forest, and KNearest Neighbors (KNN)—to identify malicious network traffic effectively. The system's methodology involves dataset preprocessing, model training, and performance evaluation using benchmark datasets such as UNSW-NB15 and CIC-IDS2017. Preliminary analysis suggests that ensemble-based models like Random Forest can achieve high detection accuracy (around 98%) with minimal computational cost. The significance of this work lies in its potential to provide a reliable, energy-efficient, and real-time security framework for military WSN applications. This paper represents the design and planning phase, with implementation and testing to be carried out in the next phase*

Keywords: Intrusion Detection, Wireless Sensor Network, Machine Learning, Cybersecurity, Military Applications, Decision Tree, Random Forest, KNN

DOI: 10.48175/IJARSCT-31157