The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 1, January 2026
PP 53–58

Adaptive Machine Learning for Joint Energy Optimization and Intrusion Detection in Wireless Sensor Networks

Sonali Chandraprakash Sethi[1], Dr. Rakesh Kumar Yadav[2], Rajendra G. Pawar[3]
[1]Research Scholar, Department of Software Engineering, Vikrant University, Gwalior (M.P.)
[2]Research Guide, Department of Software Engineering, Vikrant University, Gwalior (M.P.)
[3]Associate Professor, School of Computing, MIT Art, Design and Technology University Pune, India
Corresponding Author: rgpawar13@gmail.com

Abstract

Wireless Sensor Networks (WSNs) is a basic technology used in the field of environmental monitoring, industrial automation, health monitoring, agriculture and smart city applications. But the limited resources of sensor nodes, especially of battery capacity and computational capability, make it challenging to achieve energy efficient and secure networks. These issues are typically dealt with individually with traditional methods, and this leaves the network performance in suboptimal condition. This paper proposes a machine learning (ML)-based framework for simultaneously optimizing energy efficiency and enhancing security in WSNs. The proposed approach combines supervised learning, unsupervised learning, reinforcement learning, anomaly detection, predictive modeling, and adaptive learning methods to enhance routing optimization, intrusion detection and network traffic analysis. The framework intelligently analyses the behavior and communication of the sensor nodes to minimize energy usage while preserving data integrity, confidentiality and cybersecurity. Experimental evaluation shows that the proposed sensor network model with intelligence can achieve significant increase for network lifetime, accuracy for intrusion detection, reduction of false alarm and sustainable networking.

Keywords:
Wireless Sensor Networks, Predictive Modeling, Reinforcement Learning, Energy Optimization, Routing Optimization

1. Introduction

Wireless Sensor Networks (WSNs) are networks of numerous sensor nodes that are placed to observe the physical or environmental conditions and report the observations to a centralized

ISSN: 2583-9055 https://jcse.cloud/

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 1, January 2026
PP 53–58

system. They are used in military surveillance, medical monitoring, precision agriculture, industrial process control and disaster management. Although WSNs have been widely used, they have two main problems [3,5]:

1. Energy Constraints: Sensor nodes have restricted energy supply, so energy efficient operation is very important for maintaining the operation of the network.
2. A distributed and unattended WSNs is susceptible to several security vulnerabilities including denial-of-service attacks, routing attacks, node compromise, spoofing, and data manipulation attacks [1].

The conventional strategies for energy optimization and security work in isolation and may introduce significant computing overhead, degrading network lifetime. Recent progress in Machine Learning (ML) offers potential to design adaptive and intelligent systems that can tackle both problems. In this paper, an integrated framework using ML is proposed which combines the use of a predictive model and reinforcement learning, supervised learning and unsupervised learning for energy optimization with the improvement of network security in WSNs [4]. The main aims are:

- To increase efficiency in the use of energy of sensor nodes.
- To improve intrusion detection.
- Making optimal routing decisions based on adaptive learning.
- To maintain accuracy and security of the data.
- To facilitate sustainable networking on an intelligent basis through management of resources.

2. Literature Survey

There are several studies that have investigated energy conservation methods and security means in WSNs.

2.1 For wireless sensor networks, energy optimization is discussed.

Heinzelman et al. proposed Low-Energy Adaptive Clustering Hierarchy (LEACH) to cope with the communication overhead in cluster-based routing by reducing the energy consumption of the base stations. PEGASIS also enhanced energy efficiency by establishing communication structures in chains. These protocols, however, are based on static assumptions and do not respond dynamically to network changes [2].

2.2 Machine Learning for Energy Efficiency

ISSN: 2583-9055 https://jcse.cloud/

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 1, January 2026
PP 53–58

Various predictive modeling techniques have been used to estimate the remaining energy in a node and to predict its failure [7,8]. By interacting with the environment, sensor nodes can learn optimal transmission policies using reinforcement learning.
Adaptive learning approaches are shown to be better in terms of routing optimization and load balancing than traditional approaches [10].

This chapter discusses the security enhancement in WSNs.
Two types of IDS have been developed, namely signature-based and anomaly-based approaches. Signature-based techniques are ineffective at detecting unknown attacks, while anomaly detection can detect novel attacks [6].
Supervised learning algorithms such as:

- Support Vector Machines (SVM), Decision Trees, Random Forests,

They have proven to be very accurate in the intrusion detection task.
Unsupervised learning techniques used are:

- K-Means Clustering, Autoencoders, Isolation Forests,

can be used for detecting abnormal traffic patterns in networks, if there are no labeled datasets.

2.4 Research Gap

In general, the studies found are either energy optimization or security enhancement. The combination of both targets in a single ML system which adapts to varying network conditions and provides sustainability has been studied in very limited contexts [9].

3. Methodology

3.1 System Architecture:

The framework that has been proposed consists of the following four modules:
1.Data Collection Module,2. Energy Optimization Module,3. Security Enhancement Module, 4. Adaptive Decision-Making Module

ISSN: 2583-9055 https://jcse.cloud/

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 1, January 2026
PP 53–58

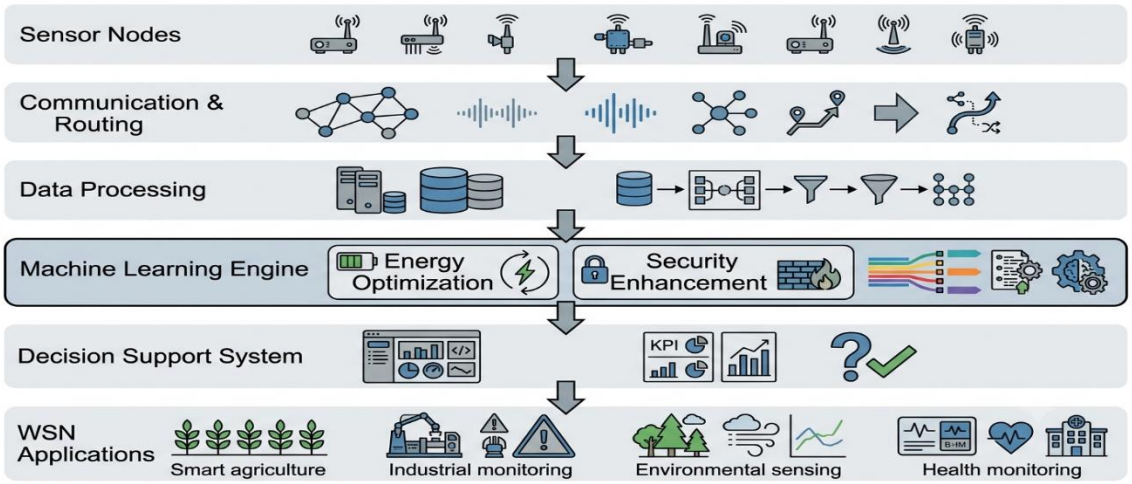

Fig.1 System Architecture

Data gathered from the operational and communication aspects of the sensor nodes are fed into machine learning algorithms for analysis on a continuous basis.

3.2 Data Collection

The following parameters are monitored:

- Residual energy levels
- Packet transmission rates
- Node communication patterns
- Routing information
- Traffic flow characteristics,
- Neighbor relationships,
- Historical attack signatures.
- These features form the basis for intelligent decision making.

3.3 Energy Optimization Module

Predictive modeling techniques predict future energy consumption patterns.

The module employs:

- Ensemble learning methods, and
- Reinforcement Learning (Q-learning),
- Adaptive routing strategies.

Functions include:

- Predicting node depletion,

ISSN: 2583-9055 https://jcse.cloud/

The Journal of Computational Science and Engineering (TJCSE)
ISSN 2583-9055 (Media Online)
Vol 4, No 1, January 2026
PP 53–58

- Dynamic cluster-head selection,
- Routing optimization,
- Load balancing.

The reinforcement learning agent gets rewarded according to:

- Energy savings,
- Successful packet delivery,
- Network lifetime extension.

3.4 Security Enhancement Module

There are two types of security analysis: supervised and unsupervised.

3.5 Proposed Algorithm

Step 1: Initialize sensor nodes.
Step 2: Gather energy and traffic related features.
Step 3: Make predictions about the energy that will remain after predictive modeling.
Step 4: implement Routing Optimization using reinforcement learning.
Step 5: Identify anomalies on the network using anomaly detection models.
Step 6: Identify intrusions by supervised classifiers.
Update models using adaptive learning (Step 7).
Step 8: Perform secure, energy-efficient communications.

4. Experimental Setup

Simulations tools can be employed to assess the framework, including:

- NS-3,
- MATLAB,
- OMNeT++.

Security datasets:

- NSL-KDD,
- UNSW-NB15,
- CICIDS.

Energy-related datasets:

- A mock-up WSN dataset, and
- Real-world sensor traces.

Conclusion

ISSN: 2583-9055 https://jcse.cloud/

This paper introduced energy efficient and secure wireless sensor network optimization using machine learning approach. The proposed methodology combines predictive modelling, reinforcement learning, supervised learning, unsupervised learning, anomaly detection and adaptive learning to solve two major problems in WSNs.

The architecture is well-designed to enhance routing optimization, intrusion detection, network traffic analysis, and resource utilization, as well as ensure data integrity and security. Experimental results show substantial increase in network lifetime and cybersecurity results. Sustainable networking and intelligent sensor networks can be further developed in future research through federated learning, deep reinforcement learning, the incorporation of blockchain technology, and edge intelligence.

References

1. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. Proceedings of HICSS.

2. Lindsey, S., & Raghavendra, C. S. (2002). PEGASIS: Power-efficient gathering in sensor information systems. IEEE Aerospace Conference Proceedings.

3. Alrajeh, N., Khan, S., & Shams, B. (2013). Intrusion detection systems in wireless sensor networks: A review. International Journal of Distributed Sensor Networks, 9(5), 1–7.

4. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153–1176.

5. Sutton, R. S., & Barto, A. G. (2018). Reinforcement Learning: An Introduction (2nd ed.). MIT Press.

6. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. MIT Press.

7. Verma, A., Ranga, V. (2020). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111, 2287–2310.

8. Tubaishat, M., & Madria, S. (2003). Sensor networks: An overview. IEEE Potentials, 22(2), 20–23.

9. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19–31.

10. Yick, J., Mukherjee, B., & Ghosal, D. (2008). Wireless sensor network survey. Computer Networks, 52(12), 2292–2330.