Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Heuristic-Optimized Machine Learning Models for Enhanced Attack Detection in Diverse Wireless Sensor Network Protocols

K. Yasotha[1*], Dr. K. Meenakshi Sundaram[2], Dr. J. Vandarkuzhali[3],

[1]Ph.D Research Scholar, PG & Research Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India. (ORCID ID: 0009-0002-2830-0702)

[2]Former Associate Professor & Head, PG & Research Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India. (ORCID ID: 0000-0003-1338-9273)

[3]Assistant Professor, PG & Research Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India. (ORCID ID: 0000-0001-5101-9404)

*Corresponding Author:pmk.yaso@gmail.com

ARTICLE INFO

Received: 29 Dec 2024

Revised: 12 Feb 2025

Accepted: 27 Feb 2025

ABSTRACT

Ensuring robust security in Wireless Sensor Networks (WSNs) is vital due to their susceptibility to various types of attacks that can compromise data integrity and network performance. This study investigates the effectiveness of machine learning models for intrusion detection across multiple WSN protocols, including TEEN, HEED, LEACH, and CFA-LEACH. Traditional classifiers such as K-Nearest Neighbors, Random Forest, Naïve Bayes, Decision Tree, and Multi-Layer Perceptron are evaluated and further enhanced through Particle Swarm Optimization (PSO) to improve detection accuracy. The research emphasizes comparative analysis across key performance metrics, demonstrating that PSO-based models offer significant improvements in classification performance. The study also explores protocol-specific attack prevalence, offering insights into the varying vulnerabilities of each protocol. The findings support the integration of swarm intelligence with machine learning as a promising approach for enhancing security and resilience in WSN environments.

Keywords: Attack Detection, WSN, Machine Learning Models, Protocol Optimization, Performance Evaluation

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are widely deployed in critical applications such as environmental monitoring, healthcare, and industrial automation, where secure and reliable communication is paramount. However, their decentralized structure and resource limitations make them highly susceptible to cyber threats, including intrusion attacks that can compromise data integrity and network stability. To address these security challenges, robust attack detection mechanisms are essential for safeguarding WSNs against malicious activities [1].

Machine learning (ML) techniques have gained prominence in intrusion detection by offering automated, data-driven classification of normal and attack traffic. Different WSN protocols, such as TEEN, HEED, LEACH, and CFA-LEACH, have

unique communication structures that necessitate adaptive and efficient detection methods. This study evaluates the performance of traditional ML classifiers and compares them with their Particle Swarm Optimization (PSO)-enhanced counterparts to assess improvements in detection accuracy and overall network security.

A comprehensive analysis is conducted across key evaluation metrics, including Accuracy, Precision, Recall, and F1-Score, to determine the effectiveness of ML models in identifying attacks within different protocols. The findings reveal that PSO-MLP outperforms all other models, demonstrating superior accuracy on the CFA-LEACH protocol, while TEEN exhibits the highest attack prevalence. The impact of PSO-based optimization in enhancing

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

classification accuracy and optimizing intrusion detection across diverse WSN environments. The paper proposes a systematic comparison of ML models for attack detection across four WSN protocols and demonstrates the impact of PSO in enhancing classification accuracy. And also identifies attack trends across protocols, aiding in tailored security strategies. By leveraging ML and optimization techniques, the research provides valuable insights into strengthening security frameworks for wireless sensor networks.

2. MATERIALS AND METHODOLOGY

The materials and methodology encompass the selection of wireless sensor network protocols, dataset preprocessing, and the application of machine learning models for attack detection. Various classifiers, including KNN, Random Forest, Naïve Bayes, Decision Tree, and Multi-Layer Perceptron, were evaluated alongside their PSO- optimized counterparts. Hyperparameter tuning was performed using PSO to enhance model performance. The classification models were assessed using key metrics such as Accuracy, Precision, Recall, and F1-Score to determine their effectiveness in detecting attacks across different network protocols.

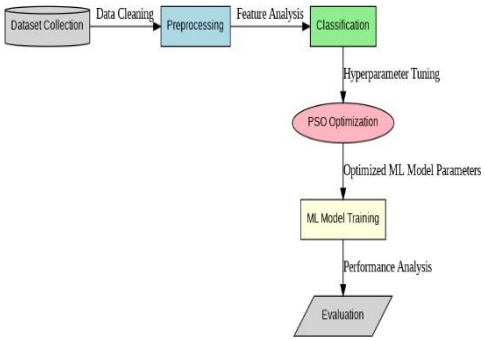


Figure 1. Proposed Optimized Machine Learning Framework

The figure represents a machine learning workflow where data undergoes preprocessing, classification, and PSO-based hyperparameter tuning before model training and evaluation to enhance performance.

2.1 Proposed Routing Protocol

LEACH uses hierarchical clustering, where Cluster Heads (CHs) aggregate and transmit data, but high CH energy depletion can be managed with SubCluster Heads (SubCHs). TEEN employs threshold-based transmission (Hard and Soft Thresholds) to reduce redundant data, making it suitable for event-driven applications but prone to data loss if thresholds are unmet. HEED selects CHs based on residual energy and communication cost, improving scalability and energy efficiency while requiring security enhancements against attacks [2].

CFA-LEACH

CFA-LEACH (Chaotic Firefly Algorithm- Optimized LEACH) is an advanced clustering protocol designed to enhance the efficiency and longevity of Wireless Sensor Networks (WSNs). It integrates the Low-Energy Adaptive Clustering Hierarchy (LEACH) with the Chaotic Firefly Algorithm (CFA) to optimize cluster head selection and energy consumption. Unlike traditional LEACH, which selects cluster heads randomly, CFA-LEACH employs an intelligent optimization mechanism based on firefly behavior, improving load balancing and reducing energy wastage. By dynamically adjusting node attractiveness, position updates, and fitness evaluations, CFA- LEACH enhances network lifetime, reduces transmission overhead, and ensures efficient data aggregation. Compared to existing protocols such as TEEN, HEED, and conventional LEACH, CFA-LEACH offers superior adaptability, lower energy consumption, and enhanced reliability, making it more effective for large-scale WSN deployments.

2.2 Classification

WSNs require efficient classification models for attack detection and route optimization to ensure network stability and security. This work integrates Particle Swarm Optimization (PSO) with a Multilayer Perceptron (MLP) to enhance classification accuracy by optimizing hyperparameters and reducing dimensionality. The PSO-MLP model is evaluated against traditional classifiers, including K-Nearest Neighbors (KNN), Random Forest (RF), Naïve

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Bayes (NB), Decision Tree (DT), and standalone MLP [5], demonstrating superior performance in detecting network anomalies while maintaining energy efficiency. Although PSO-MLP improves classification accuracy and robustness, it faces computational overhead challenges, necessitating further optimizations for real-time applications. This approach contributes to the development of resilient and scalable WSNs by addressing key issues in security, performance, and efficiency [6].

3. RESULT AND DISCUSSION

This section presents a comprehensive evaluation of various machine learning models applied to intrusion detection in wireless sensor networks. The simulated dataset, generated using OMNeT++, captures essential network transmission, timing, power, and attack classification features. Experiments were conducted using Python code on Google Colab, where models were evaluated using metrics such as Accuracy, Precision, Recall, and F1- Score [7]. The results reveal that PSO-optimized models, especially PSO-MLP, consistently outperform traditional classifiers across TEEN, HEED, LEACH, and CFA-LEACH protocols, with CFA-LEACH demonstrating the best security performance due to its lower attack rate.

3.1 Dataset Description

The dataset is generated by simulating a wireless sensor network environment using OMNeT++. The simulation is conducted for four different network protocols: TEEN, HEED, LEACH, and CFA- LEACH. Each protocol is designed to handle data transmission and energy efficiency uniquely, affecting attack patterns and normal traffic behavior. The dataset consists of 5,000 data points for each protocol, capturing network features such as packet transmission rates, energy consumption, node connectivity, and attack signatures. These features are essential for training and evaluating machine learning models in detecting malicious activities and optimizing intrusion detection across different wireless sensor network protocols.

Table.1. Network Transmission Features

Feature Name	Description
Node ID	Unique identifier for the transmitting node.
Protocol Type	The network protocol used (TEEN, HEED, LEACH, CFA-LEACH).
Packet Type	Type of packet transmitted (e.g., data, control, acknowledgment).
Packet Size (bytes)	Size of the transmitted packet in bytes.
Transmission ID	Unique identifier for each transmission.
Receiver ID	ID of the node receiving the packet.
Center Frequency (Hz)	Frequency at which the transmission occurs.
Bandwidth (Hz)	Available bandwidth for data transmission.

Table.2. Timing and Power Features

Feature Name	Description
Time (t)	Timestamp indicating when

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

	the event occurred.
Start Time	Time when the packet transmission started.
End Time	Time when the packet transmission ended.
Preamble Duration	Time duration of the preamble for synchronization.
Data Duration	Time duration of the actual data transmission.
Header Duration	Time duration of the packet header.
Transmission Power (W)	Power level used for wireless transmission.

Table.3. Attack Classification Features

Feature Name	Description
Event	Unique identifier for each recorded event.
Label (Attack/Normal)	Indicates whether the instance corresponds to an attack or normal traffic.
Attack Type	Type of attack detected (e.g., Blackhole, Flooding, Grayhole, TDMA).

These above tables define the key attributes of network transmission, timing, power, and attack classification, capturing essential features for analysing packet flow, energy consumption, and intrusion detection in wireless sensor networks [8].

This dataset, generated from the proposed CFA- LEACH protocol, simulates wireless sensor network behaviour, capturing transmission patterns, power usage, and attack instances to support intrusion detection and network optimization.

3.1 Experimental Analysis

The experimental analysis, based on comprehensive metric evaluations, confirms that optimization techniques significantly enhance model performance and overall system robustness.

Table. 4. Accuracy comparison in %

Model	TEEN	HEED	LEACH	CFA-LEACH
PSO-KNN	86.3	87.2	86.1	88.5

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

PSO-RF	92.5	91.8	91.3	94.0
PSO-NB	81.2	83.7	82.5	85.9
PSO-DT	90.4	91.1	90.2	92.7
PSO-MLP	96.8	97.2	96.5	98.1

In the above table, the accuracy comparison of ML models across different WSN protocols highlights the performance improvements achieved with PSO.

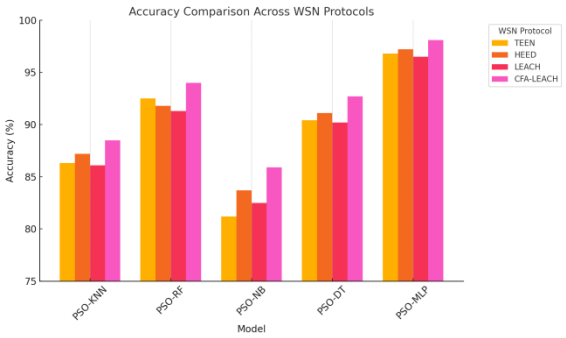


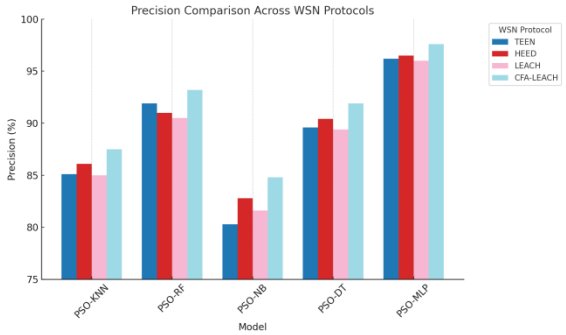
Fig 2. Accuracy Comparison

Among traditional models, MLP integrated with PSO significantly enhances classification accuracy, with PSO-MLP achieving the best results, reaching 98.1% for CFA-LEACH. The accuracy gains in PSO-based models demonstrate the effectiveness of optimization techniques in refining network intrusion detection, reducing misclassifications, and improving overall system robustness, with PSO- MLP emerging as the most efficient classification approach.

The precision comparison of ML models across different protocols, as shown in the above table and figure, highlights significant improvements with PSO-based optimization. Traditional models like MLP and RF demonstrate strong precision, with MLP reaching 92.5% for CFA-LEACH. However, the integration of PSO further refines classification accuracy, reducing misclassification rates and enhancing model reliability.

Table 5. Precision Comparison in %

Model	TEEN	HEED	LEACH	CFA-LEACH
PSO-KNN	85.1	86.1	85.0	87.5
PSO-RF	91.9	91.0	90.5	93.2
PSO-NB	80.3	82.8	81.6	84.8
PSO-DT	89.6	90.4	89.4	91.9
PSO-MLP	96.2	96.5	96.0	97.6



Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Fig 3. Precision Comparison

The proposed PSO-MLP model achieves the highest precision at 97.6%, demonstrating its effectiveness in distinguishing attack patterns from normal traffic with minimal false positives.

The recall comparison of machine learning models across different protocols highlights the effectiveness of PSO-based optimization in improving detection performance.

Table 6. Recall comparison in %

Model	TEEN	HEED	LEACH	CFA-LEACH
PSO-KNN	85.0	86.0	84.9	87.4
PSO-RF	91.8	90.8	90.4	93.1
PSO-NB	80.1	82.5	81.5	84.7
PSO-DT	89.5	90.2	89.2	91.7
PSO-MLP	96.1	96.4	95.8	97.5

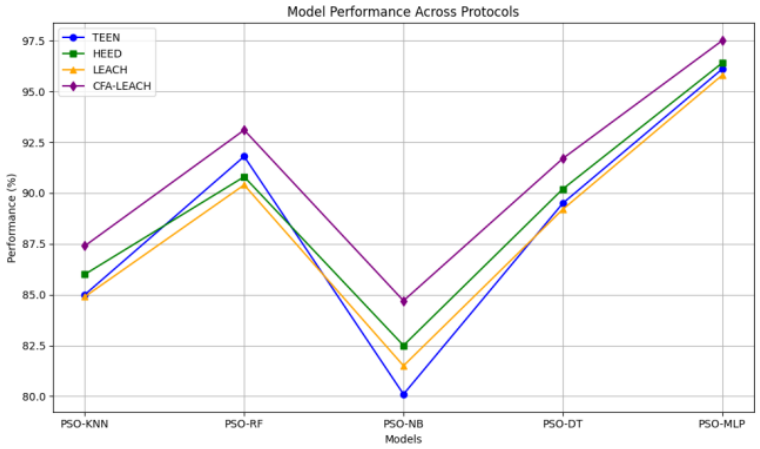


Fig 4. Recall comparison

Higher recall values indicate the model's ability to correctly identify attack instances, minimizing false negatives. The PSO-optimized models demonstrate superior recall, with PSO-MLP attaining the highest value of 97.5%, ensuring a more comprehensive detection of intrusions.

Table 7. F1-score comparison in %

Model	TEEN	HEED	LEACH	CFA-LEACH
PSO-KNN	85.1	86.0	84.9	87.4
PSO-RF	91.8	90.9	90.4	93.1
PSO-NB	80.2	82.6	81.5	84.7
PSO-DT	89.5	90.3	89.3	91.8
PSO-MLP	96.1	96.4	95.9	97.5

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

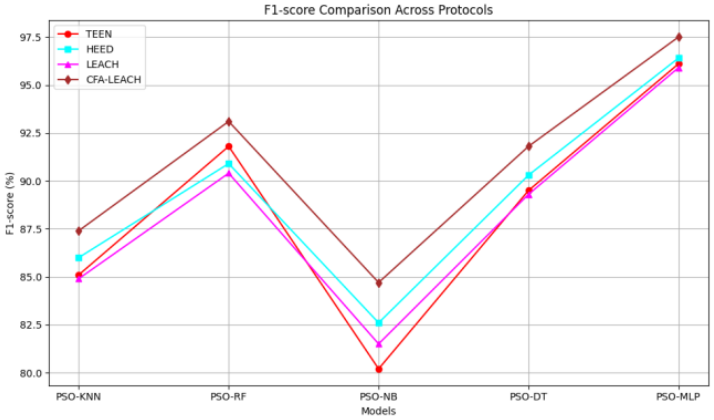


Fig. 5. F1-score comparison

The F1-score comparison of machine learning models across different protocols demonstrates the balance between precision and recall in detecting network intrusions. Higher F1-scores indicate the model's effectiveness in minimizing false positives and false negatives while ensuring accurate classification. the application of PSO significantly enhances classification accuracy, with PSO-MLP achieving the highest F1-score of 97.5%.

The proposed PSO-MLP model achieves superior performance across all protocols, with CFA- LEACH demonstrating the highest metrics (98.1% accuracy, 97.6% precision, 97.5% recall/F1-score).

Table 8. Performance of Proposed PSO-MLP Model Across WSN Protocols

Protocol	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
TEEN	96.8	96.2	96.1	96.1
HEED	97.2	96.5	96.4	96.4
LEACH	96.5	96.0	95.8	95.9
CFA-LEACH	98.1	97.6	97.5	97.5

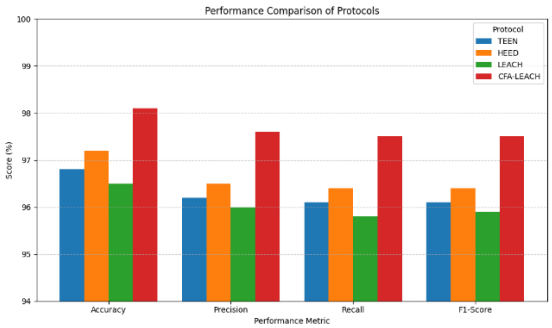


Fig.6. PSO-MLP Performance on WSN Protocols

Results highlight the effectiveness of PSO optimization and the robustness of the CFA-LEACH protocol in network intrusion detection tasks.

Journal of Information Systems Engineering and Management
2025, 10(48s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Table.9. Attack Detection across Protocols

Protocol	Total Data Points	Attack Instances (%)	Normal Instances (%)
TEEN	5,000	65%	35%
HEED	5,000	48%	52%
LEACH	5,000	50%	50%
CFA-LEACH	5,000	30%	70%

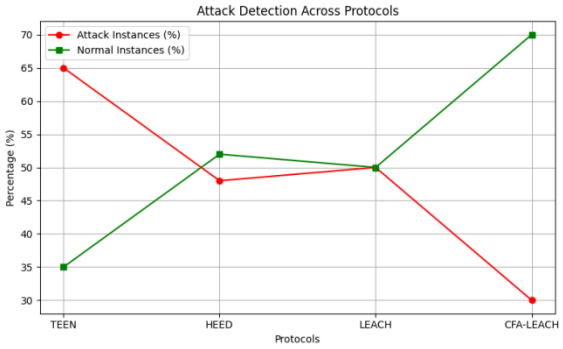


Fig.7. Attack and Normal Data Distribution across WSN Protocols

The table and figure summarize attack detection statistics for four protocols, each evaluated over 5,000 data points. TEEN shows the highest attack rate at 65%, with only 35% normal, while HEED and LEACH have nearly balanced rates at 48%/52% and 50%/50% respectively. CFA-LEACH stands out with the lowest attack rate at 30% and 70% normal instances, indicating relatively better security performance compared to the others.

4. CONCLUSION

The research paper presented a comprehensive evaluation of traditional ML models and their PSO-enhanced variants across four widely adopted WSN protocols: TEEN, HEED, LEACH, and CFA-LEACH. The results indicate that PSO significantly improves the performance of classification models across key metrics, including accuracy, precision, recall, and F1-score. The PSO-optimized Multi-Layer Perceptron (PSO-MLP), in particular, demonstrated notable performance gains over its non-optimized counterpart, highlighting the value of swarm intelligence in enhancing intrusion detection systems.

The paper also identified significant variations in attack prevalence across the protocols, with TEEN showing the highest vulnerability and CFA-LEACH exhibiting the lowest. These findings suggest that CFA-LEACH may offer better resilience against malicious activity, reinforcing its potential for secure WSN deployment. Overall, this paper confirms that integrating PSO with ML models can lead to more effective and reliable intrusion detection frameworks, contributing to the advancement of security in wireless sensor networks.

5. REFERENCES

[1] Michaelraj Kingston Roberts, Jayapratha Thangavel, Hamad Aldawsari, An improved dual-phased meta-heuristic optimization-based framework for energy efficient cluster-based routing in wireless sensor networks, Alexandria Engineering Journal, Volume 101, 2024, Pages 306-317, ISSN 1110-0168.

[2] Ghadi, Y. Y., Mazhar, T., Al Shloul, T., Shahzad, T., Salaria, U. A., Ahmed, A., & Hamam, H. (2024, January 17).

Research Article

Machine learning solutions for the security of wireless sensor networks: A review. IEEE Access.

[3] Ouchitachen, H., Hair, A., Salami, M. (2023). Heuristic Optimization of the LEACH Routing Protocol in Wireless Sensor Networks. In: Idrissi, N., Hair, A., Lazaar, M., Saadi, Y., Erritali, M., El Kafhali, S. (eds) Artificial Intelligence and Green Computing. ICAIGC 2023. Lecture Notes in Networks and Systems, vol 806. Springer, Cham.

[4] Sharma, A.; Babbar, H.; Rani, S.; Sah, D.K.; Sehar, S.; Gianini, G. MHSEER: A Meta- Heuristic Secure and Energy-Efficient Routing Protocol for Wireless Sensor Network-Based Industrial IoT. Energies 2023, 16, 4198.

[5] N. Meenakshi et al., "Efficient Communication in Wireless Sensor Networks Using Optimized Energy Efficient Engroove Leach Clustering Protocol," in Tsinghua Science and Technology, vol. 29, no. 4, pp. 985-1001, August 2024.

[6] N. Sreekanth, G. N. Babu, G. R. Kumar, M. G and A. M. Shakir, "A Cluster Based Routing Using Energy Efficiency-Based Multi- Objective Optimization in Wireless Sensor Networks," 2023 International Conference on Ambient Intelligence, Knowledge Informatics and Industrial Electronics (AIKIIE), Ballari, India, 2023, pp. 1-6.