Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 47 No. 03 (2026)

Enhanced Intrusion Detection in Wireless Sensor Networks Using PSO-Optimised Machine Learning and Deep Learning Models on Protocol-Specific Datasets

Dr. K.Yasotha [1] Dr. R. Kanakaraj[2]

[1]Assistant Professor, Department of Computer Science PPG College of Arts and Science

Coimbatore, Tamil Nadu, India
Assistant Professor, Department of Computer Science, PPG College of Arts and Science

Coimbatore, Tamil Nadu, India

Abstract: The effectiveness of Machine Learning (ML) and Deep Learning (DL) models for intrusion detection in Wireless Sensor Networks (WSNs) is highly dependent on the dataset used for training and evaluation. This paper presents a comprehensive comparative study using two distinct datasets: the benchmark Wireless Sensor Network Dataset (WSN-DS) and a custom-simulated dataset generated via OMNeT++ incorporating multiple routing protocols. We propose and evaluate a suite of models hyperparameter optimized with Particle Swarm Optimization (PSO), including PSO-MLP, against their standard counterparts (KNN, RF, NB, DT, and MLP). Our results demonstrate that while all models perform well on the generalized benchmark, the PSO-MLP model consistently achieves superior performance (up to 98.1% accuracy) on the complex, protocol-specific simulated dataset. This study highlights the critical importance of dataset selection and the significant performance gains achieved through metaheuristic optimization, providing a robust framework for developing intrusion detection systems (IDS) tailored to specific WSN architectures.

Keywords: Wireless Sensor Networks, Intrusion Detection, Particle Swarm Optimization, WSN-DS, OMNeT++, Machine Learning, Deep Learning, Comparative Analysis.

1. Introduction

WSNs have emerged as a foundational technology for applications ranging from environmental monitoring and industrial automation to military surveillance and healthcare. Despite their widespread adoption, WSNs are inherently vulnerable to security threats due to resource-constrained nodes, open wireless mediums, and distributed architectures. Among these threats, Denial-of-Service (DoS) attacks are particularly destructive, as they disrupt communication, exhaust node energy, and degrade overall network performance [1].

ML and DL models have been extensively investigated for intrusion detection in WSNs. These models are commonly developed and validated using standardized benchmark datasets such as WSN-DS, which provide clean and well-labeled samples for common attack types. While benchmark datasets enable rapid prototyping and fair algorithm comparison, they fail to capture the protocol diversity, traffic variability, and environmental complexity present in real-world WSN deployments. As a result, models demonstrating high accuracy on benchmark datasets frequently experience performance degradation in operational networks a phenomenon known as dataset shift.

To overcome this limitation, the present study introduces a systematic methodology for enhancing the robustness and generalizability of IDS in WSNs. PSO is employed to fine-tune the hyperparameters of both ML [2] and DL models [3], producing optimized classifiers such as PSO-KNN, PSO-RF, PSO-NB, PSO-DT, and PSO-MLP. These classifiers are evaluated on **two distinct datasets**:

- WSN-DS (Benchmark): A publicly available dataset representing general DoS attacks on a LEACH-based WSN [4].

- Custom OMNeT++ Dataset: A newly generated dataset simulating protocol-specific attacks on TEEN, HEED, LEACH, and the proposed CFA-LEACH protocols, providing a more realistic testing environment [5].

The key **contributions** of this work are as follows:

- Demonstration of PSO based hyperparameter optimization for enhancing ML and DL model performance.
- Comprehensive comparative analysis of baseline and optimized models across both benchmark and simulated datasets, highlighting robustness to dataset shift.
- Identification of PSO-MLP as the most effective classifier, achieving superior accuracy under diverse protocol conditions.

The remainder of this paper is organized as follows. Section 2 describes the datasets, models, and experimental setup. Section 3 presents performance results and comparative analyses across the two datasets. Section 4 concludes the study and outlines potential future research directions.

2. Literature Survey

WSN infrastructures have become increasingly vulnerable to sophisticated cyber threats, driving the development of advanced IDSs. Recent research emphasizes the effectiveness of hybrid ML and DL frameworks for robust WSN security. Al-Quayed et al. (2024) proposed a predictive framework for Industry 4.0 WSNs using the WSN-DS, combining Decision Tree (DT), Multi-Layer Perceptron (MLP), and Autoencoder models to achieve 99.52% accuracy while prioritizing threats for proactive mitigation. Similarly, Sajid et al. (2024) integrated Extreme Gradient Boosting (XGBoost) and CNN for feature extraction with LSTM classification across multiple benchmark datasets, including CIC-IDS-2017, UNSW-NB15, NSL-KDD, and WSN-DS, achieving 99.3% accuracy. CNN and LSTM based architectures, as demonstrated by Sadia et al. (2024) and Guo and Xie (2025), further highlight the capability of deep temporal and spatial feature extraction to detect complex and small-sample attacks, underscoring the advantages of hybrid and high-dimensional learning approaches in WSN intrusion detection.

Optimization and ensemble-based strategies have also been shown to significantly enhance IDS performance. Benmalek and Seddiki (2025) applied PSO to tune multiple ML and DL models on RT-IoT2022, with CatBoost + PSO achieving 98.7% accuracy. Birahim et al. (2025) combined PSO with an ensemble of Random Forest (RF), DT, and KNN, addressing class imbalance via SMOTE-Tomek and incorporating interpretability using LIME and SHAP, attaining 99.73% accuracy. Khan et al. (2024) utilized PSO based Ensemble Weighted Voting (PSO-EWV) with TabNet, SVM, and RF on WUSTL and UNSW-NB18 datasets, achieving near-perfect F-scores for MITM and Botnet detection. Additional approaches, including energy-aware routing (Lei, 2024) and fuzzy deep reinforcement learning frameworks (Khatami et al., 2025), demonstrate that optimization, explainable ensembles, and simulation-driven methods collectively improve both detection accuracy and network efficiency. These studies highlight the critical role of PSO optimized, hybrid, and explainable ML/DL frameworks, while emphasizing the importance of benchmark and custom-simulated datasets for reliable, high-performance intrusion detection in WSNs and IoT environments.

Table.1. ML/DL Based Intrusion Detection in IoT/WSN

Author(s) & Year	Dataset	ML/DL Methods	Accuracy	Limitation
Al-Quayed et al. (2024) [6]	WSN-DS	DT, MLP, Autoencoder	99.52%	High computational resources needed

Benmalek & Seddiki (2025) [7]	RT-IoT2022	SVM, KNN, CatBoost, NB, CNN, LSTM	98.7%	Limited generalization to unseen IoT networks
Birahim et al. (2025) [8]	WSN-DS	Ensemble (RF, DT, KNN)	99.73%	May be less effective in extremely large-scale or dynamic WSNs
Sajid et al. (2024) [9]	CIC-IDS-2017, UNSW NB15, NSL-KDD, WSN-DS	XGBoost, CNN, LSTM	99.3%	High dimensionality increases complexity
Khan et al. (2024) [10]	WUSTL, UNSW-NB18	TabNet, SVM, RF	99.992%	Dataset-specific; limited generalization
Lei (2024) [11]	WSN-DS	PSO with Fuzzy clustering	96.8%	Focused on energy efficiency, not security
Khatami et al. (2025) [12]	Synthetic simulation	FDRL	97.6%	Evaluated on synthetic data
Sadia et al. (2024) [13]	WSN-DS	CNN	97%	Focused on Wi-Fi WSNs only
Guo & Xie (2025) [14]	CIC-IDS-2017	TRBMA	99.88%	High model complexity
Talukder et al. (2024) [15]	WSN-DS	ML with SMOTE-TomekLink	99.92%	Limited real-time deployment discussion

3. Materials and methodology

Diverse and realistic WSN datasets are utilized to rigorously evaluate intrusion detection performance. Preprocessing ensures feature consistency and enhances model learning. Sophisticated hyper parameter optimization techniques are employed to identify optimal configurations, improving accuracy, stability, and generalization. Classification leverages advanced models capable of capturing complex temporal and spatial patterns in network traffic. The methodology establishes a robust, scalable, and high performance framework for reliable intrusion detection in heterogeneous WSN environments.

3.1. Dataset description

This work utilizes two datasets to evaluate intrusion detection performance under varying network conditions:

i. WSN-DS (Benchmark Dataset): The WSN-DS benchmark dataset, publicly available and generated using NS-2, contains 374,661 records with 19 features, capturing general DoS attacks such as Blackhole, Grayhole, Flooding, and TDMA on a LEACH based WSN. It serves as a standardized baseline for validating intrusion detection models.

ii. Simulation OMNeT++ Dataset (Proposed): The Simulation dataset, generated using the OMNeT++ simulator, comprises 5,000 records per protocol and captures protocol-specific traffic and attacks on TEEN,

HEED, LEACH, and CFA-LEACH. With features such as protocol type, transmission power, timing metrics, and attack labels, it provides a heterogeneous and realistic WSN environment for robust model evaluation.

Table.2. Comparison of Benchmark and Proposed Datasets

Feature	WSN-DS (Benchmark)	Simulation OMNeT++ (Proposed)
Origin	Pre-existing (NS-2)	Custom-simulated (OMNeT++)
Protocol	LEACH only	CFA-LEACH
Size	374,661 records	355,670 records
Scope	General DoS attacks	Protocol-specific traffic & attacks
Complexity	Lower	Higher
Realism	Standardized benchmark	Closer to real deployment

3.3. Preprocessing

Scaling is a fundamental pre-processing step in PSO optimized intrusion detection for WSNs. It standardizes numerical features, such as sensor readings and network traffic metrics, to a uniform range, preventing feature magnitude disparities from biasing the learning process. Min-max normalization is commonly applied

$$X_{scaled} = \frac{x - \min(x)}{\max(x) - \min(x)}$$

By ensuring consistent feature ranges, scaling improves model convergence, enhances the effectiveness of PSO in feature weighting, and directly contributes to higher detection accuracy, lower false positives, and robust performance on both benchmark WSN-DS and custom simulated datasets [16].

3.4. Hyper parameter tuning

Hyper parameter tuning is essential for improving model accuracy and stability. We employed Grid Search (GS), Random Search (RS), Bayesian Optimization (BO), Genetic Algorithm (GA) [17], PSO [18], and the proposed Progressive PSO with Entropy Control (PPSO-E). PPSO-E uses an adaptive entropy-based mechanism to balance exploration and exploitation, ensuring efficient parameter search. This prevents premature convergence and identifies optimal configurations. Results show PPSO-E outperforms other methods, delivering robust models.

Proposed: PPSO-E (Progressive Particle Swarm Optimization with Entropy Control)

The PPSO-E enhances optimization by adaptively balancing exploration and exploitation through dynamic parameter adjustment and entropy driven diversity control. The inertia weight decreases linearly as $w = w_{max} - \frac{w_{max} - w_{min}}{T} \cdot t$, while acceleration coefficients evolve as $c_1 = c_1^{initial} \cdot e^{-\alpha t/T}$ and $c_2 = c_2^{initial} \cdot (2 - e^{-\alpha t/T})$, allowing particles to progressively shift from global search to local refinement. Each particle updates velocity and position using $v_i^t = w \,.\, v_i^{t-1} + c_1 r_1 (p_i - x_i^{t-1}) + c_2 r_2 (g - x_i^{t-1})$ and $x_i^t = x_i^{t-1} + v_i^t$, with boundary constraints ensuring feasibility. Fitness evaluations update personal and global bests, while population entropy is computed as $H(t) = -\sum_{j=1}^{D} p_j(t) \log p_j(t)$ to monitor diversity. If entropy drops below the threshold $H_{threshold}$, exploration is reinforced to prevent premature convergence and stagnation. After completing the maximum iterations T, the algorithm outputs the global best solution g_{best}, ensuring robust convergence and reliable parameter optimization.

Pseudocode for PPSO-E

Input:

N: Swarm size, *D*: Parameter dimension, *T*: Maximum iterations, *LB*: Lower bounds, *UB*: Upper bounds, $H_{threshold}$: Entropy threshold, α: Adjustment rate

Output:

g_{best}: Optimized parameters

Begin

Initialize swarm positions x_i^0 and velocities v_i^0 for *i*=1 to *N*;

Initialize personal bests $p_i = x_i^0$ and global best g;

$t \leftarrow 1$;

while $t \leq T$ do

Update parameters:

$$w = w_{max} - \frac{w_{max} - w_{min}}{T} \cdot t$$

$$c_1 = c_1^{initial} \cdot e^{-\alpha t/T}$$

$$c_2 = c_2^{initial} \cdot (2 - e^{-\alpha t/T})$$

for each particle i do

Update velocity:

$$v_i^t = w \,.\, v_i^{t-1} + c_1 r_1 (p_i - x_i^{t-1}) + c_2 r_2 (g - x_i^{t-1})$$

Update position:

$$x_i^t = x_i^{t-1} + v_i^t$$

Apply constraints:

$$x_i^t = \max(LB, \min(UB, x_i^t))$$

Evaluate fitness:

$$f_i^t = f(x_i^t)$$

Update personal best:

if $f_i^t < f(p_i)$ then $p_i = x_i^t$

end for

Update global best g

Calculate entropy $H(t)$

if $H(t) < H_{threshold}$ then

Increase exploration;

end if

$t \leftarrow t + 1$

end while

return g

End

3.5. Classification

For intrusion detection, several classifiers were used, including K-Nearest Neighbors (KNN) [19], RF [20], Naïve Bayes (NB) [21], DT [22], and MLP [23] as baseline models. The proposed Residual Progressive MLP (RP-MLP) was developed with residual connections and progressive learning to enhance feature representation and improve classification in WSN.

Proposed: Residual Progressive MLP (RP-MLP)

The RP-MLP state prediction models residuals to improve accuracy and stability. Given historical sensor readings $\{S_1, S_2, \dots\dots, S_t\}$, a time series $H_i = s_i^{(1)}, s_i^{(2)}, \dots\dots, s_i^{(t)}$ is constructed for each sensor $i = 1, \dots\dots, d$ For $k = s$ to $t-1$, a sliding window $X_{input} = s_i^{(k-s+1)}, \dots\dots, s_i^{(k)}$ is fed into the RP-MLP to predict a residual $\hat{r}$, which is added to the last observed reading $\hat{s}_i^{(k+1)} = s_i^{(k)} + \hat{r}$. The model is trained by minimizing the mean squared error $\mathcal{L} = MSE(\hat{s}_i^{(k+1)}, target)$. After training, the latest window $X_{final} = s_i^{(t-s+1)}, \dots\dots, s_i^{(t)}$ is used to predict $\hat{r}_{t+1}$, producing $\hat{s}_i^{(t+1)} = s_i^{(t)} + \hat{r}_{\{t+1\}}$. The predictions for all sensors are aggregated as $S_{t+1} = s_1^{(t+1)}, s_2^{(t+1)}, \dots\dots, s_d^{(t+1)}$, providing a robust, sensor specific forecast that captures temporal dependencies and reduces error propagation.

Pseudocode: RP-MLP

Input: Historical sensor readings $\{S_1, S_2, \dots\dots, S_t\}$

Output: Predicted sensor readings S_{t+1}

for each sensor $i = 1, \dots\dots, d$ do

Construct time series: $H_i = s_i^{(1)}, s_i^{(2)}, \dots\dots, s_i^{(t)}$

for $k = s$ to $t-1$ do

$X_{input} = s_i^{(k-s+1)}, \dots\dots, s_i^{(k)}$

$target = s_i^{(k+1)}$

$\hat{r} = RP - MLP_{Model_i(X_{input})}$

$\hat{s}_i^{(k+1)} = s_i^{(k)} + \hat{r}$

$\mathcal{L} = MSE(\hat{s}_i^{(k+1)}, \quad target)$

Update model parameters

$X_{final} = s_i^{(t-s+1)}, \dots\dots, s_i^{(t)}$

$\hat{r}_{t+1} = RP - MLP_{Model_i(X_{final})}$

$\hat{s}_i^{(t+1)} = s_i^{(t)} + \hat{r}_{\{t+1\}}$

Return $S_{t+1} = s_1^{(t+1)}, s_2^{(t+1)}, \dots\dots, s_d^{(t+1)}$

3.6 Proposed Protocol: Choatic based firefly (CFA) algorithm

The CFA enhances the traditional Firefly Algorithm by integrating chaotic sequences to improve optimization in WSNs. Fireflies are initialized with random positions X_i and their brightness is calculated as $I_i = f(X_i)$ based on the objective function. Chaotic sequences generated via the logistic map, $x_{n+1} = rx_n(1 - x_n)$, introduce controlled randomness, improving global search and preventing premature convergence. Fireflies move toward

brighter individuals according to the attractiveness function $\beta = \beta_0 e^{-\gamma r_{ij}^2}$, with positions updated as $x_i = x_i + \beta(x_j - x_i) + \alpha \cdot$ (chaotic sequence), where α balances exploration and exploitation.

To refine solutions, CFA applies a global best Chaotic Local Search (CLS) using $\sigma_{i,j}^{k+1} = \mu\sigma_{i,j}^{k+1}(1 - \sigma_{i,j}^{k})$ and retains superior solutions. The randomization parameter α is adaptively reduced as $\alpha^{t+1} = \alpha^t(1 - t/T)$ to improve convergence. This framework efficiently identifies optimal routing paths and cluster configurations in WSNs, and when applied to PSO-optimized intrusion detection, it enhances feature selection, parameter tuning, detection accuracy, and overall performance on both benchmark (WSN-DS) and custom-simulated datasets.

4. Result and Discussion

This section presents a comprehensive analysis of classifiers and PSO optimized models for intrusion detection in WSN. It evaluates model performance using key metrics such as accuracy, recall, precision, and F1-score to assess detection capability and reliability. The discussion highlights the comparative effectiveness of different approaches and the impact of optimization strategies on improving network security. Insights from this analysis provide guidance for selecting robust and efficient models for intrusion detection.

4.1 Performance Metrics

The performance of PSO optimized models for intrusion detection in WSN is evaluated using the following metrics, where TP = True Positives, TN = True Negatives, FP = False Positives and FN = False Negatives

Table.3. Performance Metrics

Metrics	Expression
Accuracy	$\frac{TP + TN}{TP + TN + FP + FN}$
Recall	$\frac{\text{TP}}{\text{TP} + \text{FN}}$ x100
Precision	$\frac{TN}{TP + FP}$
F1-Score	$2.\frac{Precison * Recall}{Precision + Recall}$

These metrics measure the correctness, detection capability, and balance between Precision and Recall of the models, providing a comprehensive assessment of their intrusion detection performance.

Table.4. Performance Comparison of ML Models on WSN-DS and Simulation Datasets

Model	WSN-DS Dataset				Simulation Dataset			
	Accuracy	Recall	Precision	F1-Score	Accuracy	Recall	Precision	F1-Score
KNN	0.90	0.91	0.89	0.90	0.91	0.92	0.90	0.91
RF	0.94	0.95	0.93	0.94	0.95	0.95	0.94	0.95
NB	0.80	0.86	0.78	0.80	0.81	0.86	0.79	0.81
DT	0.85	0.84	0.86	0.85	0.86	0.85	0.86	0.86
MLP	0.95	0.96	0.94	0.95	0.96	0.96	0.95	0.96
RP-MLP	**0.96**	**0.96**	**0.95**	**0.96**	**0.97**	**0.97**	**0.96**	**0.97**

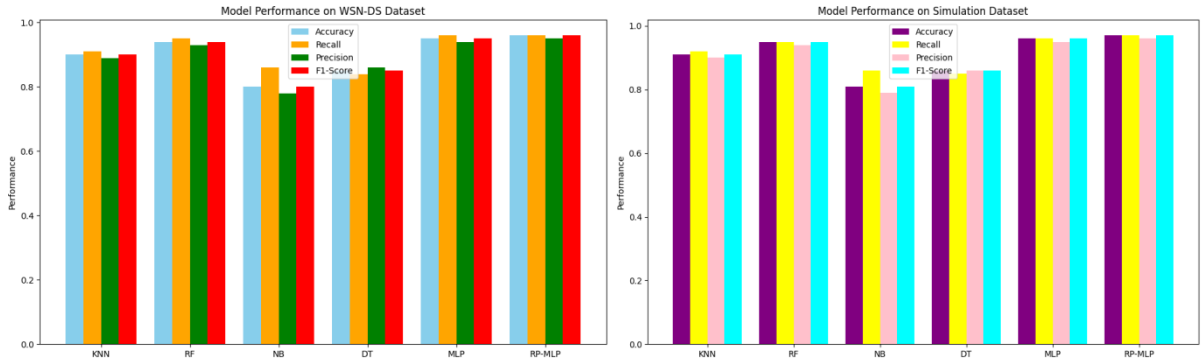

Fig.1. ML Model Performance on WSN-DS & Simulation Datasets

The above table and graph describe performance comparison of models on the WSN-DS benchmark and simulation dataset shows that classical methods such as KNN, RF, NB, and DT achieve moderate results, with RF consistently performing better among traditional approaches. Deep learning models demonstrate superior accuracy, where MLP achieves 0.95 on WSN-DS and 0.96 on the simulation dataset. The proposed RP-MLP further outperforms all models, reaching 0.96 accuracy on WSN-DS and 0.97 on the simulation dataset with balanced precision, recall, and F1-scores, highlighting its robustness and reliability for intrusion detection in WSN.

Table.5. Hyperparameter Tuning Comparison of Optimization Models on WSN-DS and CFA-LEACH

Model	WSN-DS Dataset				Simulation Dataset			
	Accuracy	Recall	Precision	F1-Score	Accuracy	Recall	Precision	F1-Score
GS	0.97	0.97	0.96	0.97	0.96	0.96	0.95	0.96
RS	0.97	0.97	0.96	0.97	0.96	0.96	0.95	0.96
BO	0.96	0.97	0.95	0.96	0.95	0.96	0.94	0.95
GA	0.97	0.98	0.96	0.97	0.96	0.97	0.95	0.96
PSO	0.98	0.98	0.98	0.98	0.97	0.97	0.97	0.97
PPSO-E	**0.99**	**0.99**	**0.98**	**0.99**	**0.98**	**0.98**	**0.97**	**0.98**

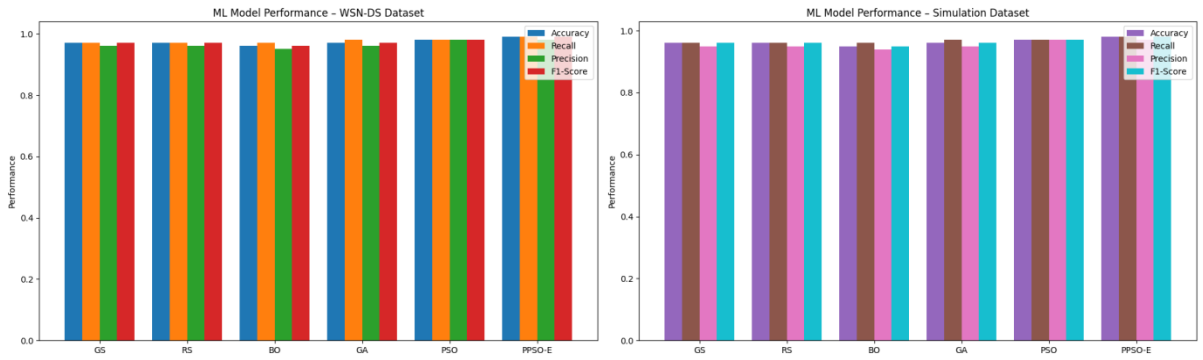

Fig.2. ML Model Performance – WSN-DS & Simulation

The above table and graph compares the performance of GS, RS, BO, GA, PSO, and the proposed PPSO-E on the WSN-DS and CFA-LEACH datasets using Accuracy, Recall, Precision, and F1-Score. On WSN-DS, GS, RS, and

GA achieved 0.97 Accuracy with 0.96 Precision, BO slightly lower at 0.96 Accuracy, PSO reached 0.98 across all metrics, while PPSO-E obtained the best results with 0.99 Accuracy, Recall, and F1-Score, and 0.98 Precision. On CFA-LEACH, GS, RS, and GA recorded 0.96 Accuracy with 0.95–0.96 Precision, BO at 0.95 Accuracy, PSO achieved 0.97 consistently, and PPSO-E again outperformed with 0.98 Accuracy and Recall, 0.97 Precision, and 0.98 F1-Score, confirming its superiority for intrusion detection in WSN.

5. Conclusion

In conclusion, this paper presents a comprehensive analysis of PSO-optimized models for intrusion detection in Wireless Sensor Networks (WSNs), highlighting the critical influence of dataset selection and optimization strategies on detection performance. The proposed RP-MLP model achieved 0.96 accuracy on the benchmark WSN-DS dataset and 0.97 on the custom-simulated OMNeT++ dataset, demonstrating that the simulated dataset produces performance comparable to the standardized WSN-DS benchmark. Hyper parameter optimization using the Progressive PSO with Entropy Control (PPSO-E) further enhanced performance, achieving 0.99 accuracy on WSN-DS and 0.98 on the simulated dataset, by effectively balancing exploration and exploitation and preventing premature convergence. This study underscores the importance of realistic, protocol-specific datasets and the significant performance gains achieved through metaheuristic optimization, providing a robust framework for developing IDS tailored to diverse WSN architectures. Overall, the integration of RP-MLP with PPSO-E establishes a scalable, high-performance, and resilient framework capable of delivering reliable intrusion detection across both benchmark and custom-simulated WSN environments, setting a benchmark for future IDS research.

References:

[1] Trinh Thuc Lai, Tuan Phong Tran, Jaehyuk Cho, Myungsik Yoo, DoS attack detection using online learning techniques in wireless sensor networks, Alexandria Engineering Journal, Volume 85, 2023, Pages 307-319, ISSN 1110-0168.

[2] M. A. Elsadig, "Detection of Denial-of-Service Attack in Wireless Sensor Networks: A Lightweight Machine Learning Approach," in IEEE Access, vol. 11, pp. 83537-83552, 2023,

[3] Shakya, Vandana & Choudhary, Jaytrilok & Singh, Dhirendra. (2024). IRADA: integrated reinforcement learning and deep learning algorithm for attack detection in wireless sensor networks. Multimedia Tools and Applications. 83. 1-20. 10.1007/s11042-024-18289-7.

[4] Ha, Asmaa & Gunawan, Teddy & Habaebi, Mohamed & Halbouni, Murad & Kartiwi, Mira & Ahmad, Robiah. (2022). CNN-LSTM: Hybrid Deep Neural Network for Network Intrusion Detection System. IEEE Access. PP. 1-1. 10.1109/ACCESS.2022.3206425.

[5] Papan, J.; Bridova, I.; Filipko, A. Design of a Technique for Accelerating the WSN Convergence Process. Sensors 2023, 23, 8682.

[6] Al-Quayed, F., Ahmad, Z., & Humayun, M. (2024). A situation-based predictive approach for cybersecurity intrusion detection and prevention using machine learning and deep learning algorithms in wireless sensor networks of Industry 4.0. IEEE Access, 12, 34800–34819.

[7] Benmalek, M., & Seddiki, A. (2025). Particle swarm optimization-enhanced machine learning and deep learning techniques for Internet of Things intrusion detection. Data Science and Management. ISSN 2666-7649.

[8] Birahim, S. A., Paul, A., Rahman, F., Islam, Y., Roy, T., Hasan, M. A., Haque, F., & Chowdhury, M. E. H. (2025). Intrusion detection for wireless sensor network using particle swarm optimization based explainable ensemble machine learning approach. IEEE Access, 13, 13711–13730.

[9] Sajid, M., Malik, K. R., Almogren, A., et al. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. Journal of Cloud Computing, 13, 123.

[10] Khan, Q. W., Khan, A. N., Ahmad, R., Rizwan, A., Ibrahim, M., & Kim, D. H. (2024). Enhanced abnormality detection via PSO-driven adaptive ensemble weighting for energy AIoT device security. IEEE

Access, 12, 138483–138500.

[11] Lei, C. (2024). An energy-aware cluster-based routing in the Internet of Things using particle swarm optimization algorithm and fuzzy clustering. Journal of Engineering and Applied Sciences, 71, 135.

[12] Khatami, S. S., Shoeibi, M., Salehi, R., & Kaveh, M. (2025). Energy-efficient and secure double RIS-aided wireless sensor networks: A QoS-aware fuzzy deep reinforcement learning approach. Journal of Sensor and Actuator Networks, 14, 18.

[13] Sadia, H., Farhan, S., Haq, Y., Sana, R., Mahmood, T., Bahaj, S., & Rehman, A. (2024). Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach. IEEE Access, PP, 1–1.

[14] Guo, D., & Xie, Y. (2025). Research on Network Intrusion Detection Model Based on Hybrid Sampling and Deep Learning. Sensors, 25, 1578.

[15] Talukder, M. A., Sharmin, S., & Uddin, M. A., et al. (2024). MLSTL-WSN: machine learning-based intrusion detection using SMOTE-Tomek in WSNs. International Journal of Information Security, 23, 2139–2158.

[16] Salmi, S., Oughdir, L. Performance evaluation of deep learning techniques for DoS attacks detection in wireless sensor network. J Big Data 10, 17 (2023).

[17] Isaac Kofi Nti, Sidharth Sankar Rout, Jones Yeboah, An optimized ensemble model for predicting average localization error of wireless sensor networks, Decision Analytics Journal, Volume 12, 2024, 100510, ISSN 2772-6622.

[18] Bhargavi, K.V.N.A.; Varma, G.P.S.; Hemalatha, I.; Dilli, R. An Enhanced Particle Swarm Optimization-Based Node Deployment and Coverage in Sensor Networks. Sensors 2024, 24, 6238.

[19] Mohamed Zaki, Ahmed & Abdelhamid, Abdelaziz & Ibrahim, Abdelhameed & Eid, Marwa & El-kenawy, El-Sayed. (2023). Enhancing K-Nearest Neighbors Algorithm in Wireless Sensor Networks through Stochastic Fractal Search and Particle Swarm Optimization. Journal of Cybersecurity and Information Management. 13. 76-84. 10.54216/JCIM.130108.

[20] Xiaoqiang Liu, Mingxue Li, Yufeng Zhang, Xiwen Zhu, Yuesheng Guan, Self-Powered wireless sensor node based on RF energy harvesting and management combined design, Energy Conversion and Management,

[21] Volume 292, 2023, 117393, ISSN 0196-8904.

[22] Singh, Davinder & Charan, Piyush & Pasrija, Divij & Shyamal, Dhananjay & Suresh, K. & Priya, Veeraraghavan. (2024). An Energy Efficient Naïve Bayes-based Clustering Protocol for Wireless Sensor Network. 1-6. 10.1109/IATMSI60426.2024.10502529.

[23] Gao, Yongli & Wang, Gang. (2024). Evaluation on Data Transmission in Wireless Sensor Networks Based on Computer Technology. International Journal of High Speed Electronics and Systems.34. 10.1142/S012915642440010X.

[24] E, G., S, S. An optimized intrusion detection model for wireless sensor networks based on MLP-CatBoost algorithm. Multimed Tools Appl 83, 66725–66755 (2024).