International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

Check for updates

Performance analysis of heuristic-optimized machine learning and swarm intelligence for secure and energy-efficient WSNs

K. Yasotha *, K. Meenakshi Sundaram and J. Vandarkuzhali

PG & Research Department of Computer Science, Erode Arts and Science College, Erode, Tamil Nadu, India.

International Journal of Science and Research Archive, 2025, 16(03), 1279-1286

Publication history: Received on 17 August 2025; revised on 26 September 2025; accepted on 30 September 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.3.2705

Abstract

Wireless Sensor Networks (WSNs) are widely used in applications such as environmental monitoring, healthcare, and industrial automation, but they face critical challenges of security vulnerabilities and limited energy resources. The study proposes a unified framework that combines machine learning–based intrusion detection with swarm intelligence–driven routing optimization to address these dual concerns. Intrusion detection is enhanced through heuristic optimization, where Particle Swarm Optimization (PSO) fine-tunes classifiers like Multi-Layer Perceptron (MLP), achieving high accuracy with low false alarm rates. On the routing side, clustering protocols such as LEACH, HEED, and TEEN are optimized using the Chaotic Firefly Algorithm (CFA), extending network lifetime, improving throughput, and reducing latency. By integrating these layers, the framework effectively isolates malicious nodes while ensuring balanced energy consumption, delivering a resilient and sustainable solution for next-generation WSN deployments.

Keywords: Wireless Sensor Networks; Intrusion Detection; Swarm Intelligence; Routing Optimization; Energy Efficiency

1. Introduction

Wireless Sensor Networks (WSNs) have become an essential technology for applications in smart cities, healthcare, industrial automation, and environmental monitoring. Their distributed sensing capability, scalability, and adaptability make them a core component of modern Internet of Things (IoT) systems. However, the design of WSNs is constrained by limited energy supply, processing power, and bandwidth, making them highly vulnerable to a wide range of attacks, including denial-of-service (DoS), blackhole, and sinkhole intrusions. Ensuring reliable performance in such environments requires approaches that can simultaneously address energy efficiency and robust security [1][2].

Recent research has explored the integration of machine learning (ML) and swarm intelligence to mitigate these challenges. ML-based Intrusion Detection Systems (IDS) have shown significant promise in detecting anomalies and attacks in WSN traffic, particularly when enhanced with heuristic optimization to improve classifier accuracy and reduce false alarms . On the other hand, energy-aware routing protocols, such as LEACH, HEED, and TEEN, can be optimized using metaheuristic algorithms like the Chaotic Firefly Algorithm (CFA) to extend network lifetime and improve throughput [2]. Building on these directions, this study presents a comprehensive framework that combines heuristic-optimized ML intrusion detection with swarm intelligence–based routing strategies to enhance both the security and sustainability of next-generation WSNs[3][4].

* Corresponding author: K. Yasotha

2. Related Work

Yasotha K, K. Meenakshi Sundaram proposes a model uses a variety of optimization techniques, including grid search, random search, Bayesian optimization, genetic algorithms, and particle swarm optimization (PSO), to focus on hyperparameter tuning of machine learning algorithms like KNN, Random Forest, Naive Bayes, Decision Trees, and Multilayer Perceptron. According to the findings, hyperparameter tuning greatly increases detection accuracy; models such as RF and MLP can achieve up to 96% and 98% accuracy, respectively[10]

Yasotha K, K.Meenakshi Sundaram, J.Vandarkuzhali introduces integrated approach with conventional routing protocols with a swarm intelligence algorithms, like the Chaotic-Based Firefly Algorithm (CFA), are. Existing protocols like TEEN, HEED, and LEACH are routinely surpassed by the suggested CFA-LEACH protocol in a number of metrics, such as packet delivery ratio, energy consumption, latency, throughput, and network lifetime. By lowering energy consumption, it extends network operation times, which is essential for extending the life of sensor nodes[11].

Yasotha K, K.Meenakshi Sundaram, J.Vandarkuzhali proposed a framework that blends swarm intelligence-driven routing optimization with machine learning-based intrusion detection. The swarm intelligence algorithms like the Chaotic Firefly Algorithm (CFA) have been integrated with routing strategies. These approaches improve cluster-head selection, enhance throughput, and extend network lifetime under both normal and adversarial conditions[12].

3. System Architecture

The proposed system architecture is designed to simultaneously enhance intrusion detection capabilities and maintain energy efficiency in Wireless Sensor Networks. At its foundation, the architecture integrates lightweight intrusion detection modules, energy-aware routing protocols, and heuristic optimization techniques into a cohesive framework that can adapt across different WSN environments.

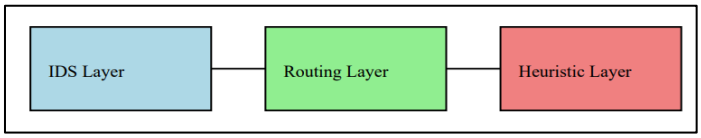

Figure 1 System Architecture for Secure and Energy Efficient WSN

The Intrusion Detection Layer is responsible for monitoring traffic patterns and identifying malicious activity. Machine learning classifiers, such as Random Forest, Decision Trees, and Multi-Layer Perceptrons, are deployed at cluster heads or base stations. These models are fine-tuned using heuristic optimization techniques like Particle Swarm Optimization (PSO) and Genetic Algorithms (GA), which improve detection accuracy while keeping computational costs manageable [6].

The Routing Optimization Layer focuses on extending network lifetime by improving energy consumption and load balancing. Classical clustering protocols such as LEACH, HEED, and TEEN are enhanced with swarm intelligence methods, including the Chaotic Firefly Algorithm (CFA)[7]. This enables efficient cluster-head selection and dynamic routing decisions, distributing energy use evenly across the network and reducing node failures caused by uneven energy depletion.

Finally, the Heuristic Integration Layer bridges security and energy efficiency by coordinating the outputs of the IDS and routing protocols. Nodes suspected of compromise are avoided during routing, while heuristic optimization continuously adjusts system parameters to maintain a balance between detection performance and energy conservation. This cooperative mechanism ensures that the network remains resilient against attacks without compromising its operational lifetime [13].

4. Methodology

The methodology adopted in this analysis combines machine learning–based intrusion detection with swarm intelligence–driven routing optimization, supported by heuristic algorithms for model tuning and system adaptability. The process begins with dataset preparation and simulation setup, followed by classifier selection and optimization, and finally the integration of routing protocols with intrusion detection.

4.1. Dataset Preparation

To evaluate detection performance, we employed the WSN-DS dataset containing hundreds of thousands of records that represent both benign and malicious traffic, including Blackhole, Grayhole, Flooding, and TDMA attacks. For energy and routing analysis, the OMNeT++ simulator was used to model different wireless sensor network topologies and routing behaviors. These simulations captured key parameters such as packet delivery ratio, throughput, latency, and energy consumption. By combining real datasets with simulation traces, the evaluation provided a balanced view of both attack detection and protocol performance.

4.2. Classifier Design and Optimization

Multiple classifiers, including k-Nearest Neighbor (KNN), Random Forest (RF), Naïve Bayes (NB), Decision Trees (DT), and Multi-Layer Perceptrons (MLP), were evaluated for their suitability in detecting intrusions. To maximize detection performance, hyperparameter tuning was applied using both conventional search methods (grid search, random search, Bayesian optimization) and metaheuristic algorithms such as Genetic Algorithm (GA) and Particle Swarm Optimization (PSO). Among these, PSO proved especially effective for tuning neural networks, resulting in the PSO-MLP model that achieved the highest accuracy with minimal false alarms[8].

4.3. Routing Protocol Optimization

To address energy efficiency, classical routing protocols such as LEACH, HEED, and TEEN were implemented and enhanced using the Chaotic Firefly Algorithm (CFA)[7]. This approach provided an adaptive cluster-head selection strategy that balanced energy usage across the network and improved resilience against node failures. The optimized routing layer was further integrated with the IDS to reroute traffic around nodes flagged as suspicious, thereby combining energy-aware communication with proactive attack mitigation[9].

4.4. Integration Strategy

The final step was to unify the optimized classifiers with the routing protocols into a cohesive system. This integration ensured that detection alerts influenced routing decisions in real time, while swarm intelligence maintained balanced energy distribution. The system thus achieved dual objectives: accurate and adaptive intrusion detection along with improved network lifetime and performance.

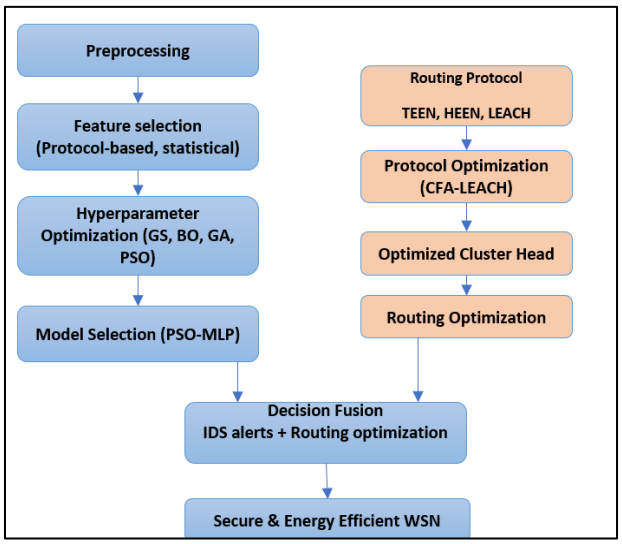

Figure 2 Integration of Optimized ML classifiers and Optimized Routing Protocol

5. Experimental Setup

The experimental evaluation was carried out through a combination of simulation environments and machine learning platforms. For intrusion detection, the WSN-DS dataset was preprocessed and analyzed using Python on Google Colab, which provided a scalable environment for training and tuning machine learning models. For routing protocol analysis, OMNeT++ was employed to simulate wireless sensor networks under varying node densities and traffic conditions, allowing the study of protocol behavior in realistic network scenarios.

Performance metrics were carefully chosen to reflect both security and energy perspectives. For IDS evaluation, metrics included accuracy, precision, recall, F1-score, and false alarm rate. For routing evaluation, network lifetime, throughput, latency, and energy consumption were measured. By combining these datasets and simulations, the experimental setup provided a holistic view of how the proposed system balances intrusion detection effectiveness with energy efficiency in WSNs.

6. Results and Analysis

The results of the paper demonstrate the integration of heuristic-optimized machine learning models with swarm-intelligent routing protocols significantly enhances both security and energy efficiency in Wireless Sensor Networks. In terms of intrusion detection, the Particle Swarm Optimization–tuned Multi-Layer Perceptron (PSO-MLP) outperformed all baseline classifiers, achieving an accuracy of over 98%. This improvement was accompanied by higher precision and recall, indicating that the model was effective at minimizing both false positives and false negatives. Compared to traditional approaches, the PSO-MLP consistently provided more reliable detection across diverse attack scenarios.

Table 1 Intrusion Detection performance on optimized MLClassifier with PSO

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
KNN	93	93	95	93
RF	96	96	96	95
NB	82	81	85	80
DT	90	90	89	88
MLP	98	98	98	98

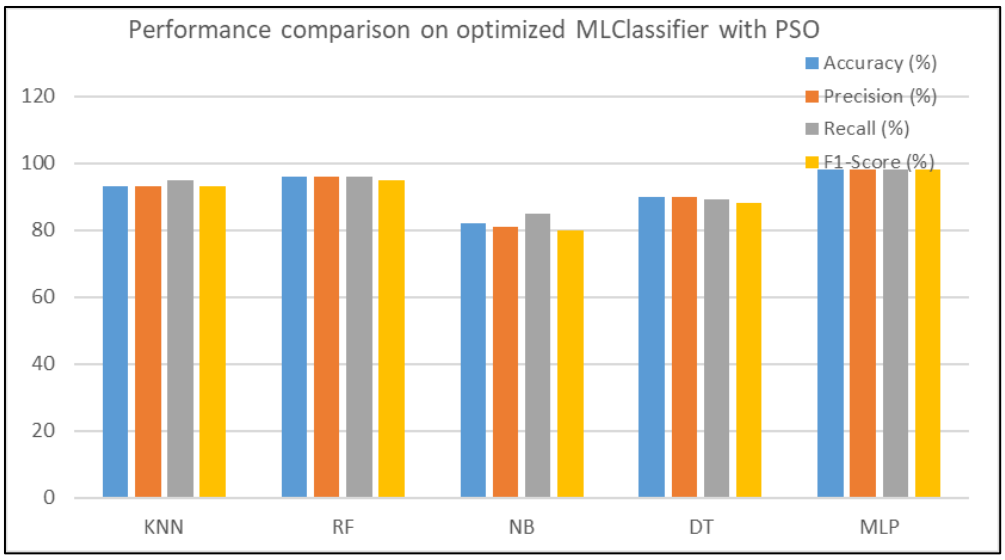

Figure 3 Performance comparison on optimized MLClassifier with PSO

The evaluation of routing protocols revealed that the Chaotic Firefly Algorithm–enhanced LEACH (CFA-LEACH) achieved the best balance between energy efficiency and compared to standard LEACH and achieved 15–20% higher throughput while reducing latency by nearly 25%.

Table 2 Performance of CFA-LEACH Routing Protocol

Metric	LEACH	HEED	TEEN	CFA-LEACH
PDR (Packet Delivery Ratio)	0.70	0.80	0.85	0.95
Throughput	0.60	0.75	0.80	0.90
End-to-End Delay	0.70	0.60	0.90	0.80
Energy Efficiency	0.40	0.60	0.55	0.85
Network Lifetime	0.40	0.60	0.60	0.85

These results show the effectiveness of swarm intelligence in addressing the uneven energy depletion problem inherent in traditional clustering protocols. HEED and TEEN also performed reasonably well but were consistently outperformed by the CFA-enhanced protocol.

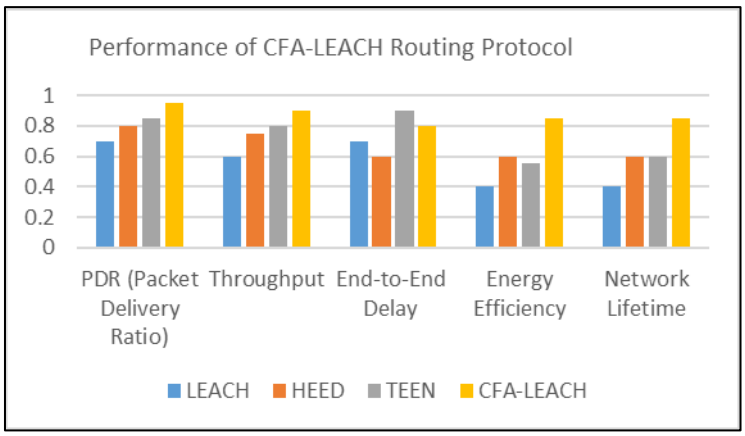

Figure 4 Performance of CFA-LEACH Routing Protocol

When the intrusion detection system was integrated with the optimized routing framework, the system maintained high levels of detection accuracy while preserving network performance.

Table 3 Performance comparison of the Proposed PSO-MLP Model Across WSN Protocols on a Simulation Dataset (CFA-LEACH)

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

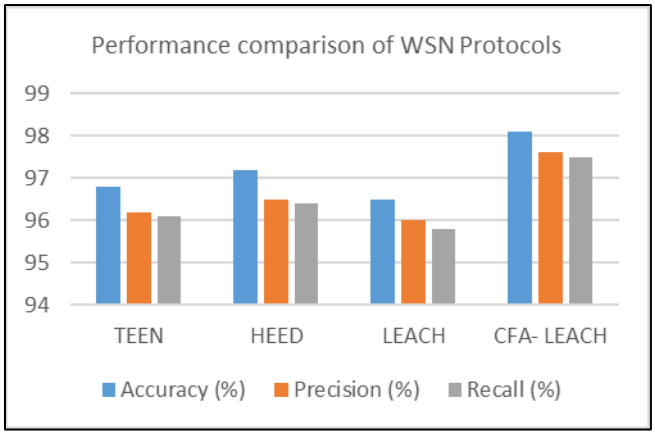

Figure 5 Performance Comparison of WSN Protocols

The PSO-MLP provides superior adaptability across protocols. Future directions include reducing computational overhead for real-time deployments, incorporating deep learning, and adversarial robustness testing. . The results highlight the synergy of combining heuristic-optimized ML IDS with swarm-intelligence-based routing. While IDS enhances attack resilience, CFA-LEACH maintains network longevity.

Table 4 and Figure 5 represent the attack deduction on the simulation dataset.The CFA-LEACH demonstrates the lowest attack incidence (30%) among the four protocols, highlighting its resilience against malicious activities compared to TEEN (65%) and LEACH/HEED (50%). This improvement arises from its optimized cluster-head (CH) selection and secure routing paths, which reduce the network's vulnerability surface.

Table 4 Attack Detection across Protocols on Simulated Dataset(CFA-LEACH)

Protocol	Total Data Points	Attack Instances(%)	Normal Instance (%)
TEEN	5000	65	35
HEED	5000	48	52
LEACH	5000	50	50
PSO-MLP CFA-LEACH	5000	30	70

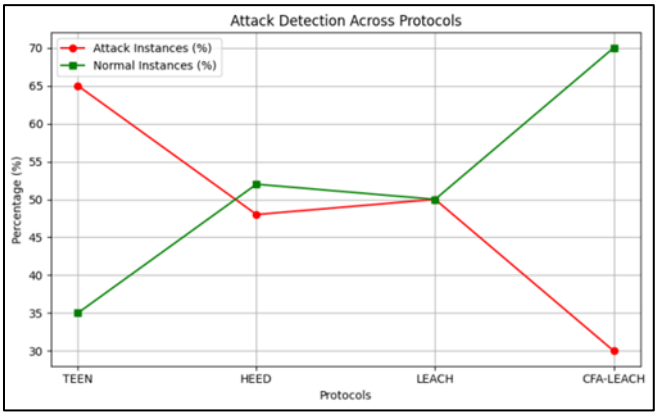

Figure 6 Attack Detection across Protocols on Simulated Dataset(CFA-LEACH)

The CFA-LEACH can be integrated with machine learning-based intrusion detection systems (e.g., PSO-MLP, Random Forest), enabling early isolation of suspicious nodes and minimizing compromised routes. With 70% of its traffic classified as normal, CFA-LEACH provides more trustworthy data delivery to the sink, enhancing packet delivery ratio, throughput, and accuracy for applications such as healthcare and environmental monitoring. Finally, its swarm

intelligence-driven adaptability allows CFA-LEACH to re-cluster dynamically under attack conditions, ensuring sustainable operation, whereas LEACH and HEED struggle due to static or random cluster-head elections.

Table 5 Performance comparison of attack deduction two datasets

Dataset	Total Data Points	Attack Instances(%)	Normal Instances (%)
WSN-DS (Optimized PSO-MLP)	73506	8	92
Simulation Dataset (PSO-MLP + Optimized LEACH)	5000	30	70

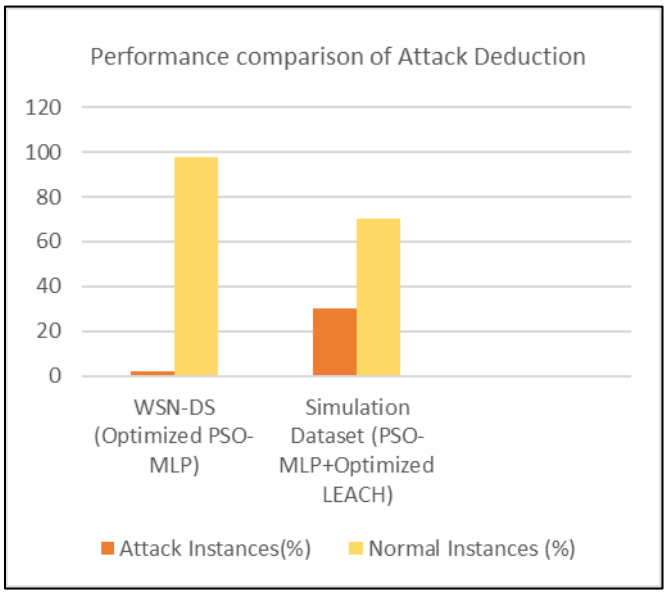

Figure 7 Performance comparison of attack deduction two datasets

The results highlight the effectiveness of different experimental setups in reducing attack incidence and improving the reliability of wireless sensor networks. On the WSN-DS dataset (Optimized PSO-MLP), the model processed 73,506 total data points, where only 8% were attack instances and 92% were normal instances. This indicates that the optimized PSO-MLP classifier achieves high precision and robustness when applied to a large-scale benchmark dataset, significantly reducing the proportion of malicious traffic. While the proportion of attacks is higher compared to the WSN-DS setup, the results demonstrate how integrating PSO-MLP with an optimized routing protocol (LEACH enhanced with swarm intelligence) still provides substantial resilience against attacks. Together, these outcomes show that combining machine learning with optimized clustering and routing strategies strengthens both attack detection and overall network trustworthiness across different experimental environments.

7. Conclusion

The paper analyses the performance of a unified framework that integrates machine learning–based intrusion detection with swarm intelligence–driven routing optimization for Wireless Sensor Networks. By leveraging heuristic optimization, particularly Particle Swarm Optimization (PSO), the framework enhances the accuracy of classifiers, such as Multi-Layer Perceptron (MLP), while maintaining a lightweight deployment suitable for resource-constrained nodes. Simultaneously, the application of the Chaotic Firefly Algorithm (CFA) to routing protocols such as LEACH significantly extended network lifetime, reduced latency, and enhanced throughput. The PSO-MLP model consistently achieved more than 98% accuracy in detecting diverse attacks, outperforming baseline classifiers. Likewise, CFA-LEACH improved network performance by 25%, proving that swarm intelligence can effectively mitigate the limitations of deterministic protocols. The integration of intrusion detection with routing optimization further reinforced system resilience by ensuring that nodes flagged as suspicious were avoided in routing decisions, thereby reducing the overall impact of attacks.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Almomani, B. Al-Kasassbeh, A. Al-Momani, and M. Alauthman, "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks," *Journal of Sensors*, vol. 2016, pp. 1–16, 201

[2] Alsulaiman L and S. Al-Ahmadi, "Performance Evaluation of Machine Learning Techniques for DoS Detection in Wireless Sensor Network," *arXiv preprint arXiv:2104.01963*, Apr. 2021.

[3] Bharti P.R and R. D. Patidar, "A Swarm Intelligence Based Clustering Technique with Scheduling for the Amelioration of Lifetime in Sensor Networks," *Wireless Personal Communications*, vol. 103, no. 3, pp. 2191–2208, 2018.

[4] Bekal P, P. Kumar, and P. R. Mane, "A Metaheuristic Approach for Hierarchical Wireless Sensor Networks using Particle Swarm Optimisation-based Enhanced LEACH Protocol," *IET Wireless Sensor Systems*, vol. 14, no. 3, pp. 134–146, 2024.

[5] Heinzelman W, A. Chandrakasan, and H. Balakrishnan, *"Energy-Efficient Communication Protocol for Wireless Microsensor Networks (LEACH),"* Proceedings of the 33rd Annual Hawaii International Conference on System Sciences (HICSS), 2000.

[6] J. Zhang, H. Chen, and Y. Liu, "Intrusion Detection Model for Wireless Sensor Networks Based on MC-GRU," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, 2022.

[7] Mirjalili S,*"The Firefly Algorithm: Theory, Literature Review, and Application in Optimization Problems,"* Nature-Inspired Metaheuristic Algorithms, Springer, 2019.

[8] Verma A and V. Ranga,[3] *"Machine Learning Based Intrusion Detection Systems for IoT Applications,"* Wireless Personal Communications, vol. 111, pp. 2287–2310, 2020.

[9] X. Li, Y. Zhang, and F. Wang, "An Energy-Efficient Data Aggregation Clustering Algorithm for Wireless Sensor Networks Using Hybrid PSO," *Energies (MDPI)*, vol. 16, no. 5, pp. 2487–2502, 2022.

[10] Yasotha K, K. Meenakshi Sundaram, "Machine Learning-Based Intrusion Detection for Mitigating Denial of Service Attacks in Wireless Sensor Networks", *International (IEEE) Conference on Self-Sustainable Artificial Intelligence Systems* (ICSSAS) at M.P Nachimuthu M. Jaganathan Engineering College, Erode held on 18-20 October 2023.

[11] Yasotha K, K.Meenakshi Sundaram, J.Vandarkuzhali, "Optimizing Energy Efficiency and Network Performance in Wireless Sensor Networks: An Evaluation of Routing Protocols and Swarm Intelligence Algorithm", *International Journal of Computational and Experimental Science and Engineering* (IJCESEN) ISSN:2149-9144, Vol.11.1, pp. 71-77, 2025.

[12] K.Yasotha , K.Meenakshi Sundaram, J.Vandarkuzhali, "Heuristic-Optimized Machine Learning Models for Enhanced Attack Detection in Diverse Wireless Sensor Network Protocols", *Journal of Information Systems Engineering and Management* ISSN: 2468-4376, Vol. 10(48s), 2025.

[13] Zhou, Y., Wang, L., & Xiao, W, "Design and implementation of intrusion detection system based on machine learning in wireless sensor networks" IEEE Access, 8, 148207-148215, 2020.