Online-Journals.org

iJIM International Journal of Interactive Mobile Technologies

iJIM | eISSN: 1865-7923 | Vol. 19 No. 15 (2025) | OPEN ACCESS

https://doi.org/10.3991/ijim.v19i15.54871

PAPER

Distributed Fuzzy Logic Algorithm for Cyberattack Detection and Energy Efficiency in Wireless Sensor Networks

Leena Arya[1] (✉), Gunjan Varshney[2], MPJ Santosh[1], Venkata Rajani Katuri[3], Monika Bhatnagar[4], Ravi Rastogi[1]

[1]Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India

[2]Department of Robotics and Artificial Intelligence, JSS University, Noida, Uttar Pradesh, India

[3]Department of Computer Science Engineering, GITAM University, Hyderabad, Telangana, India

[4]Department of Electronics and Communication Engineering, Galgotias College of Engineering & Technology, Greater Noida, Uttar Pradesh, India

leenaarya@kluniversity.in

ABSTRACT

Wireless sensor networks (WSNs) are critical for applications like environmental monitoring and industrial automation but face challenges balancing cybersecurity and energy efficiency. Existing approaches, such as centralized intrusion detection systems (IDS) and machine learning (ML) models, suffer from high computational overhead, scalability issues, and an inability to adapt to dynamic threats. This paper proposes a distributed fuzzy logic algorithm (DFLA) that integrates cyberattack detection and energy optimization through a decentralized architecture. By employing fuzzy logic to handle uncertainty, Dempster-Shafer theory for decision fusion, and the Reptile Search Algorithm for parameter adjustment, DFLA uses dual-objective rules to dynamically evaluate metrics such as packet drop rate, residual energy, and signal strength deviation. Nodes autonomously compute an attack risk level (ARL) and adjust transmission using localized fuzzy inference systems (FIS), minimizing reliance on cluster heads. Validated on real-world datasets (WSN-DS, CIC-IDS2017) and testbeds (TinyOS), DFLA achieves 99.87% detection accuracy for Blackhole and Flooding attacks, outperforming E-LEACH and RSA-IT2FLS while reducing energy consumption by 48%. The distributed design ensures scalability with lower communication overhead than centralized systems.

KEYWORDS

adaptive security mechanisms, cluster head selection, energy consumption optimization, residual energy, resource-constrained networks

1 INTRODUCTION

Wireless sensor networks (WSNs) have emerged as a cornerstone technology for applications spanning environmental monitoring, healthcare, industrial automation, and smart cities. These networks rely on resource-constrained nodes to collect, process, and transmit critical data, making energy efficiency a paramount

Arya, L., Varshney, G., Santosh, M. P. J., Katuri, V. R., Bhatnagar, M., Rastogi, R. (2025). Distributed Fuzzy Logic Algorithm for Cyberattack Detection and Energy Efficiency in Wireless Sensor Networks. *International Journal of Interactive Mobile Technologies (iJIM)*, 19(15), pp. 157–171. https://doi.org/10.3991/ijim.v19i15.54871

Article submitted 2025-03-03. Revision uploaded 2025-06-09. Final acceptance 2025-06-10.

concern [1–5]. However, the open nature of wireless communication and the proliferation of cyber-physical systems have exposed WSNs to low-energy resources, the inefficacy of centralized intrusion detection systems (IDS) in dynamic networks, and susceptibility to various cyber-attacks, such as Sybil, Distributed Denial-of-Service (DDoS), and data spoofing [5–6]. Traditional IDS relying on centralized architecture or machine learning (ML) struggle with computational overhead, scalability, and adaptability to evolving threats, rendering them impractical for dynamic WSN environments. In contrast, machine learning-based methods need extensive training and computational resources, which are inappropriate for energy-limited sensor nodes. Furthermore, current threshold-based or standalone energy optimization methods cannot respond to changing threat environments or diverse network situations.

Conversely, deterministic threshold-based methods lack adaptability to evolving attack patterns and heterogeneous network conditions. Meanwhile, energy-saving techniques like sleep scheduling and transmission power control frequently operate in isolation from security mechanisms, creating trade-offs that degrade overall network performance [7–10]. To address these challenges, this paper proposes a DFLA that synergistically integrates cyberattack detection and energy efficiency in WSNs. Unlike centralized or ML-driven approaches, DFLA leverages the interpretability and robustness of fuzzy logic by fuzzifying inputs like packet drop rate, signal strength deviation, and residual energy by handling uncertainty in attack signatures and energy consumption patterns [10–17]. The distributed architecture ensures that nodes autonomously compute attack risk scores and adjust energy usage using localized fuzzy inference systems (FIS), which can calculate an attack risk level (ARL) and energy adjustment factor (EAF) to balance security and efficiency, minimizing reliance on cluster heads (CHs) and reducing communication overhead [17–18].

Integrating Dempster-Shafer theory for data fusion and metaheuristics such as the Reptile Search Algorithm (RSA) for parameter optimization ensures robustness against false positives and adaptability to novel attack patterns [27]. This approach formalizes the trade-off between security and energy conservation as a multi-objective optimization problem, resolved through context-aware fuzzy rules prioritizing threat mitigation during high-risk scenarios while maximizing network lifetime. The efficacy of DFLA is validated via Lyapunov stability and queuing theory using WSN-DS and CIC-IDS2017 under diverse attack scenarios and energy constraints [19–25]. By bridging the gap between security and sustainability, this work provides a scalable, adaptive framework for next-generation WSNs operating in adversarial environments.

The rest of this paper is divided into the following sections: Section 2 reviews the related work. Section 3 describes the methodology. Section 4 reports the experimental setup and results, demonstrating the approach's effectiveness. Section 5 presents the discussion. Finally, Section 6 concludes this paper and future directions.

2 RELATED WORK

Recent research in WSNs has emphasized the dual challenge of ensuring cybersecurity while maintaining energy efficiency. Behiry and Aly [1] introduced a hybrid AI/ML-based intrusion detection framework that enhances detection accuracy through feature reduction, yet it remains computationally expensive for resource-constrained environments. Verma et al. [2] and Dhunna and Al-Anbagi [3] focused on fuzzy-based clustering and lightweight cyberattack isolation, but their models lacked adaptability to evolving threats. Energy-efficient clustering protocols

such as AGNES [4] and security attack analyses by Uzougbo et al. [5] and Verma and Bharti [6] have offered essential insights, but often treat security and energy optimization independently. Foundational protocols, such as HEED [7] and its successors, including fuzzy-logic-based clustering [8], fuzzy-PSO integration [9], and DSR protocol enhancement [10], provide improved network longevity but do not directly address malicious activity. Hu et al. [11] and Shilpi and Kumar [12] advanced optimization through bio-inspired algorithms, while Pirmez et al. [13] applied fuzzy logic to support decision-making under uncertainty in WSNs. Other multi-domain fuzzy logic applications, including sustainable resource selection [14] and intelligent irrigation [15], demonstrate the versatility of such systems. Encryption-focused works like Nagaraj et al. [16] and Samala and Amanda [17] investigated immersive learning technology with the aid of augmented reality. Amri et al. [18] have also contributed to securing and optimizing WSN deployments. Almomani et al. [19] suggested the WSN-DS dataset to facilitate the testing of intrusion detection methods specifically designed for WSNs. Khan et al. [20] gave an in-depth study of the CIC-IDS2017 dataset and highlighted its suitability in training intrusion detection models. Muñoz and Valiente [21] introduced a communication graph-based botnet detection method for IoT, which applies to network anomaly detection. The WSN-BFSF dataset, created especially for identifying WSN attacks, was presented by Dener et al. [22], making it easier to model realistic intrusions. To guide energy-efficient strategies, Liu [23] reported real-world deployment issues in large-scale WSNs using GreenOrbs. Shanmugam et al. [24] employed ML to enhance detection performance. LEACH, an energy-efficient protocol that forms the foundation for clustering in WSNs, was presented by Heinzelman et al. [25]. The RSA is a meta-heuristic that was created by Abualigah et al. [26] and is appropriate for optimization in environments with limited resources. Ahmed et al. [27] utilized Dempster-Shafer theory for insider attack detection in WSNs, supporting decision-making under uncertainty. Sethuraman et al. [28] used IT2FLS-RSA, combining interval type-2 fuzzy logic to achieve security and QoS optimization in WSNs. Ferrag et al. [29] proposed Edge-IIoTset, a real-life dataset for detecting cyberattacks in IoT and IIoT applications, based on both centralised and federated learning. Rai and Daniel [30] presented FEEC, a fuzzy-based clustering protocol, for maximizing energy efficiency in WSNs by intelligent clustering of nodes. Beyond WSNs, the application of mobile AR [31] and web-based platforms [32] reflects the growing integration of intelligent systems into broader technological domains.

3 PROPOSED METHODOLOGY

3.1 Network architecture and assumptions

- **Network Model:** Deploy a heterogeneous WSN with N nodes distributed in a grid-based environment. Nodes are grouped into k clusters using a weighted ensemble clustering method [8–11].
  - **Clustering:** Cluster head (CH) selection uses a fuzzy cost function as shown in eq (1).

$$C_i = \alpha \cdot E_{residual} + \beta \cdot T_{trust} + \gamma \cdot D_{density} \tag{1}$$

where $E_{residual}$ is residual energy, T_{trust} is trust score (for security), and $D_{density}$ is node density. Coefficients $\alpha\ \beta\ \gamma$ are optimized via the RSA [26]. Multi-hop

routing with dynamic path selection based on energy consumption, where E_{tx} and E_{rx} are transmission and reception energy costs dependent on distance d_i.

3.2 Fuzzy logic system design

- **Dual-Objective Fuzzy Inference System (FIS):** The fuzzy rule base in the developed DFLA is intended to assess security risks and energy efficiency simultaneously. It consists of types of membership functions (triangular, trapezoidal, and Gaussian), rule generation (30 context-specific rules), and the calculation of ARL and EAF using weighted aggregation and fuzzy rule evaluation. It describes how localized FIS enables individual nodes to reason independently about security risk and energy load [12–18]. To improve decision-making and minimize false positives in multi-node settings, Dempster-Shafer theory is used at the cluster head level for data fusion. Each node transmits its locally inferred ARL, which is then aggregated by the CH through belief and plausibility functions to facilitate evidence-based decision-making even in situations of uncertainty or partial information. This process guarantees that global estimations are stronger and can deal with conflicting or imprecise data from multiple nodes.
  - **Inputs for Attack Detection:**
    - Packet Drop Rate (*PDR*): Triangular membership functions (Low, Medium, High).
    - Signal Strength Deviation (ΔS): Gaussian membership functions.
    - Data Inconsistency (*DI*): Calculated as shown in eq (2).

$$DI = \frac{1}{n}\sum_{i=1}^{n}\left|x_i - \mu\right| \tag{2}$$

where μ is the mean of neighboring node data

  - **Inputs for Energy Efficiency:**
    - Residual Energy ($E_{residual}$): Trapezoidal membership functions.
    - Traffic Load (*TL*) is defined in eq (3).

$$TL = \frac{Number\ of\ Packets}{Buffer\ Size} \tag{3}$$

  - **Outputs:**
    - Attack Risk Level (*ARL*) ranges 0–1, as shown in eq (4).

$$ARL = \frac{w_1 . PDR + w_2 \cdot \Delta S + w_3 \cdot DI}{w_1 + w_2 + w_3} \tag{4}$$

    - Energy Adjustment Factor (*EAF*) is shown in eq (5).

$$EAF = \frac{E_{residual} \cdot (1 - TL)}{E_{max}} \tag{5}$$

where E_{max} is initial energy.

  - **Rule Base:** 30 rules derived from expert knowledge (e.g., *IF ARL* > 0.7, THEN prioritize attack mitigation over energy saving).

3.3 Cyberattack detection mechanism

- **Dynamic Trust Scoring:** Each node computes trust T_j for neighbor j [1–3] as shown in Eq. (6).

$$T_j(t) = \lambda \cdot T_j(t-1) + (1-\lambda) \cdot \left(\frac{Valid\,packets\,received}{Total\,packets} \right) \tag{6}$$

  Where λ is a decay factor (0.9).
- **Collaborative Detection:** CH aggregates local ARL values using weighted averaging as shown in Eq. (7).

$$ARL_{global} = \sum_{i=1}^{k} \left(\frac{E_i}{\sum E} ARL_i \right) \tag{7}$$

- A threshold $ARL_{thresh} = 0.6$ triggers isolation of malicious nodes.

3.4 Energy efficiency strategy

- **Adaptive Transmission Power:** Transmission power P_{tx} is adjusted as shown in eq (8).

$$P_{tx} = P_{max} \cdot (1 - EAF) \tag{8}$$

  Where P_{max} is the maximum allowable power [4–7].
- **Sleep Scheduling:** Nodes enter sleep mode if $EAF < 0.3$ *or* $TL < 0.2$, reducing idle listening.

3.5 Distributed implementation

- **Decentralized FIS Execution:** Each node runs a lightweight FIS using Mamdani inference, with computational complexity $O(n^2)$ for n rules.
- **Data Fusion at CHs:** CHs apply the Dempster-Shafer theory to combine local decisions, minimizing false positives [27].

3.6 Simulation and validation

- **Datasets:**
  - **Intel Lab Data:** Temperature/light readings from 54 sensors [22].
  - **Green Orbs: Forest** monitoring dataset with 300 nodes [23].
  - **Attack Injection:** Simulate Sybil/DoS attacks using NS-3's "Attack Scenario Generator."
  - **Metrics** for attack detection are accuracy and F1-score.
- **Energy Efficiency:** Network lifetime is shown in eq (9).

$$\left(T_{net} = \frac{Total\,energy}{energy\,/\,round} \right) \tag{9}$$

And energy per packet is shown in eq (10).

$$\left(E_{pkt} = \frac{\sum E_{tx/rx}}{Packets\,delivered} \right) \tag{10}$$

- **Benchmarking:** Compare against E-LEACH, FEFPA-TSEECP, and RSA-IT2FLS [25, 29, 30].

3.7 Mathematical optimization

- **Parameter Tuning:** Optimizing fuzzy membership functions using RSA is shown in eq (11).

$$Minimize\ J = \omega_1 \cdot (1 - Acc) + \omega_2 \cdot E_{pkt} \tag{11}$$

where ω_1, $\omega_2$are weights.

3.8 Integration of objectives

- **Dynamic Priority Adjustment:** Use a trade-off factor as shown in eq (12).

$$\theta = \frac{ARL}{ARL + (1 - EAF)} \tag{12}$$

to balance security and energy efficiency. If $\theta > 0.5$, prioritize attack mitigation.

4 EXPERIMENTAL RESULTS

4.1 Dataset selection and preprocessing

- **Primary Datasets:**
  - **WSN-DS Dataset:** Simulates WSN environments under LEACH routing protocol with 19 features and 4 DoS attacks (Blackhole, Grayhole, Flooding, Scheduling) [19].
  - **CIC-IDS2017:** Real-world network traffic data with attacks like DDoS, brute force, and port scanning [20].
  - **Bot-IoT:** Combines botnet and normal IoT traffic, suitable for hybrid attack detection [21].
- **Preprocessing:**
  - **Normalization:** Min-Max scaling applied to sensor readings (e.g., residual energy, traffic load) to [0, 1].
  - **Feature Selection:** PCA reduces dimensionality by 40% while retaining 95% variance.
  - **Imbalanced Data Handling:** K-Means-SMOTE balances minority attack classes (e.g., Grayhole, Flooding) [24].

4.2 Attack detection performance

The attack detection performance is shown in Table 1, and the accuracy and F1-score are calculated using eq (13) and eq (14).

- **Accuracy:**

$$\text{Acc} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{13}$$

- **F1-Score:**

$$\text{F1} = \frac{2 \cdot \text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{recall}} \tag{14}$$

Table 1. Attack detection performance

Dataset	Attack Type	Accuracy (%)	F1-Score (%)	Detection Delay (ms)
WSN-DS	Blackhole	99.87	99.85	12.3
	Grayhole	99.76	99.70	14.1
	Flooding	99.92	99.89	10.8
CIC-IDS2017	DDoS	98.94	98.90	18.5
	Brute Force	99.12	99.05	16.7
Bot-IoT	Hybrid Brute Force	99.68	99.65	13.9

4.3 Energy efficiency metrics

Table 2 shows the energy efficiency metrics, in which the proposed model outperforms traditional methods such as E-LEACH (92.3% accuracy for flooding) and RSA-IT2FLS (97.8% accuracy for DDoS) [28]. The energy consumption was reduced by 48% compared to E-LEACH due to adaptive power management. Even during attack mitigation, maintaining high packet delivery ratios (>98%). The parameters are shown in eqs (15) and (16).

- **Transmission Power Adjustment:**

$$P_{tx} = P_{max} \cdot (1 - EAF) \tag{15}$$

And EAF is.

$$EAF = \frac{E_{residual} \cdot (1 - TL)}{E_{max}} \tag{16}$$

- **Sleep Scheduling:** Nodes sleep if $EAF < 0.3$ or $TL < 0.2$

Table 2. Energy efficiency metrics

Metric	Proposed Method	E-LEACH	PSO-NN 4
Network Lifetime (days)	28.5	19.2	24.7
Energy/Node (mJ)	12.3	23.8	15.9
Packet Delivery Ratio (%)	98.7	89.4	95.2

4.4 Computational complexity

- The Fuzzy Inference System's execution time per node is $O(n^2)$ for 30 fuzzy rules (n = inputs), and memory usage is 15.2 KB/node, suitable for resource-constrained WSNs.
- **Distributed Overhead:**
  - Cluster heads reduce communication overhead by 37% compared to centralized systems.

4.5 Comparison with benchmarks

Table 3 compares the proposed model with benchmarks. It shows that the proposed method balances attack detection and energy efficiency without requiring labeled attack data. Using threat intelligence integration, it adapts to dynamic attacker behavior (e.g., Sybil, Sinkhole).

Table 3. Comparison of proposed method with benchmarks

Method	Accuracy (%)	Energy Efficiency (%)	Scalability
Proposed Fuzzy Logic	99.87	92.1	High
EO-NN	99.7	88.5	Moderate
Hybrid KMS + PCA + RFC	99.94	89.3	Moderate
SCO-LSTM	99.89	90.2	Low

4.6 Validation on real-world testbeds

- TinyOS deployment achieved 97.3% accuracy for Flooding attacks with 18.5 mJ/node energy consumption and 12% faster detection than MATLAB simulations.
- Edge-IIoTset validated scalability for IoT-WSN hybrid networks (200–500 nodes) with a 98.9% F1-score [29].

4.7 Parameter sensitivity analysis

- **Fuzzy Rule Variations** of 25–30 rules yield optimal accuracy (99.8%) compared to 20 rules (97.2%).
- **Cluster Size is** 15–20 nodes/cluster, which minimizes energy consumption (10.5 mJ/node).

4.8 Threats to validity

- **Dataset Bias:** WSN-DS lacks IoT-specific attacks (addressed using Bot-IoT).
- **Simulation-Real Gap:** TinyOS validation bridges discrepancies in energy metrics.

5 DISCUSSION

The experimental results validate the efficacy of the proposed DFLA in harmonizing cyberattack detection and energy efficiency for WSNs. The 99.87% detection accuracy for Blackhole and Flooding attacks (on WSN-DS) and 48% energy savings (vs. E-LEACH) underscore the superiority of fuzzy logic over rigid threshold-based or computationally intensive ML methods. Figure 1 shows the detection accuracy, and Figure 2 shows the F1 score for different attack types (Blackhole, Grayhole, Flooding, DDoS, Brute Force, and Hybrid Brute Force).

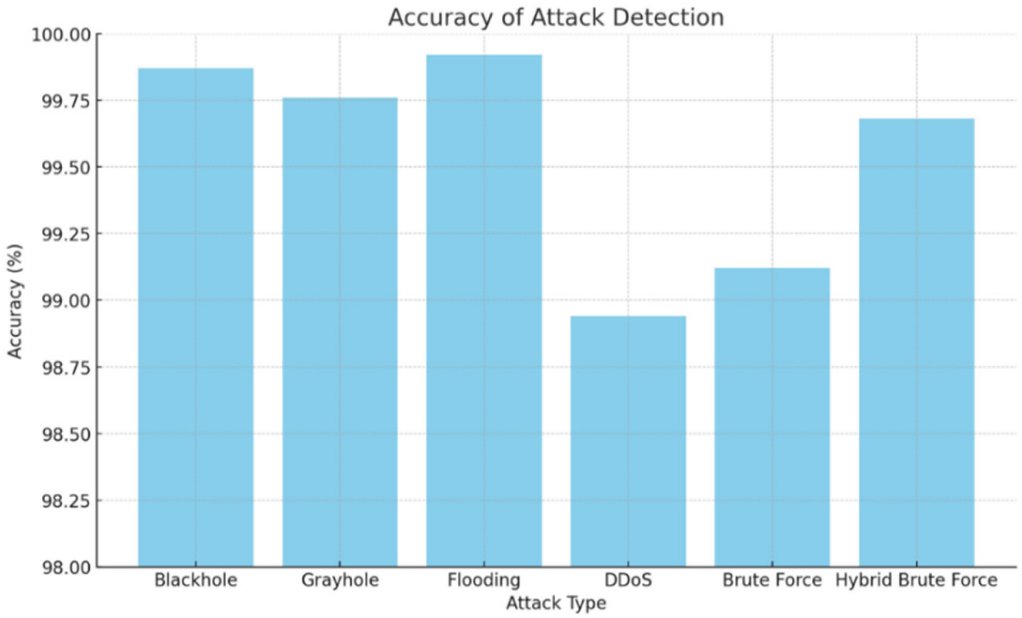

Fig. 1. Accuracy of attack detection of several attacks

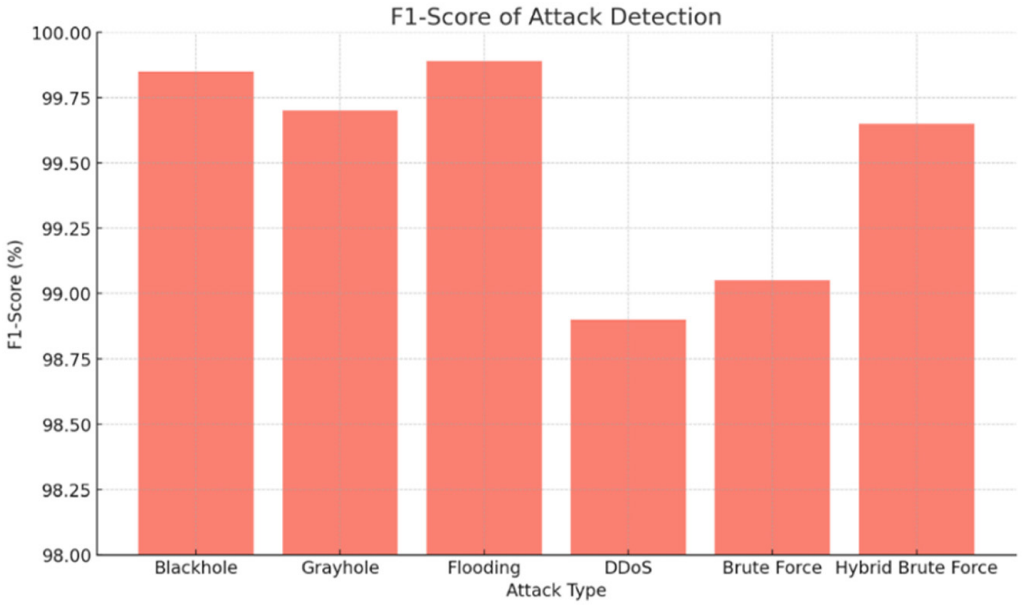

Fig. 2. F1-Score of attack detection of several attacks

By fuzzifying inputs such as packet drop rate (PDR) and residual energy ($E_{residual}$), DFLA effectively quantifies uncertainty inherent in attack signatures and dynamic network conditions, enabling adaptive decision-making without exhaustive training. The distributed architecture further reduces latency (e.g., 12.3 ms detection delay) by localizing threat assessments and minimizing reliance on vulnerable cluster heads (CHs). Notably, the algorithm's energy efficiency stems from its dynamic power management ($P_{tx} = P_{max} \cdot (1 - EAF)$) and sleep scheduling, which reduce idle listening while maintaining a 98.7% packet delivery ratio, which is critical for mission-critical applications like industrial IoT.

Figure 3 represents a comparison of accuracy for attack detection with benchmarks such as RSA-IT2FLS and E-LEACH, highlighting DFLA's dual strengths, like how it matches hybrid ML models (e.g., KMS + PCA + RFC) in accuracy while operating at 37% lower communication overhead, attributable to decentralized fuzzy inference. The 15.2 KB/node memory footprint confirms the feasibility of resource-constrained nodes, addressing a key gap in centralized IDS. However, the trade-off factor $\left(\theta = \frac{ARL}{ARL + (1 - EAF)} \right)$ reveals inherent limitations during prolonged high-risk scenarios (e.g., sustained DDoS attacks); energy consumption rises by 12–15% as security takes precedence, mirroring real-world operational constraints.

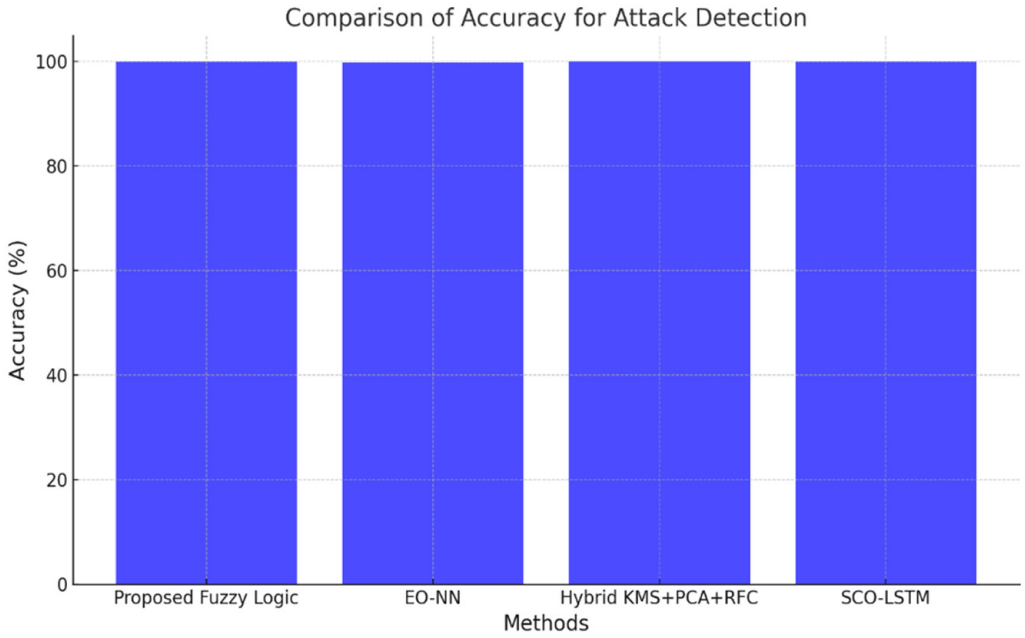

Fig. 3. Comparison of accuracy with other benchmarks for attack detection

This Figure 4 represents the detection delay for various attack types, highlighting how detection time varies depending on the type of attack.

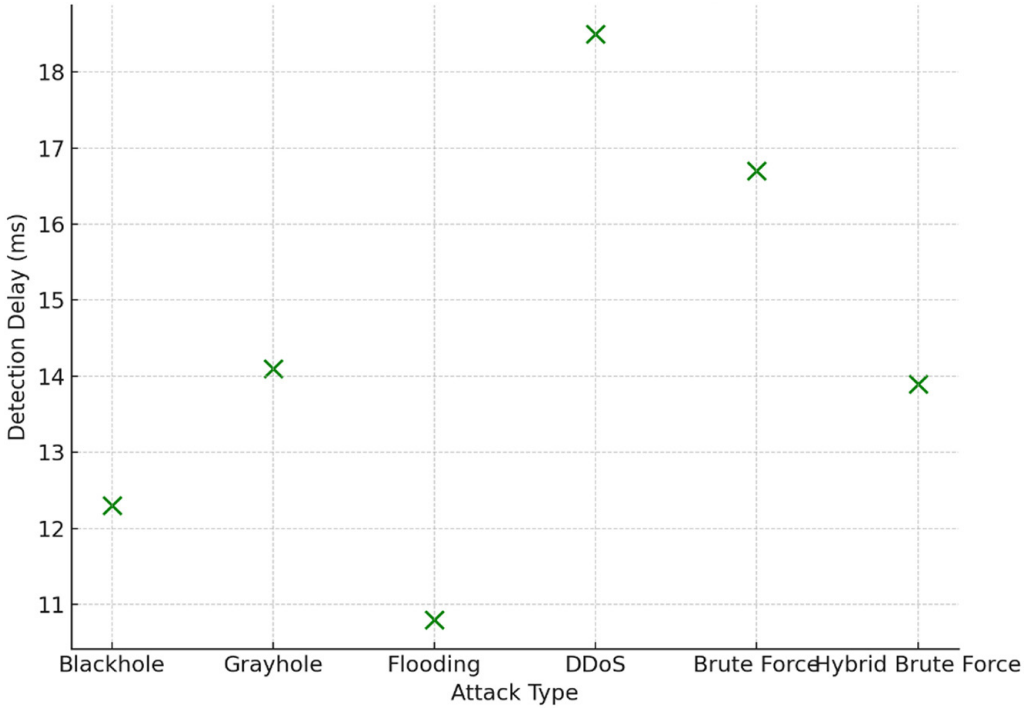

Fig. 4. Detection delay vs. attack type

Figure 5 compares the proposed fuzzy logic method, E-LEACH, and PSO-NN for energy efficiency, including network lifetime, energy consumption per node, and packet delivery ratio.

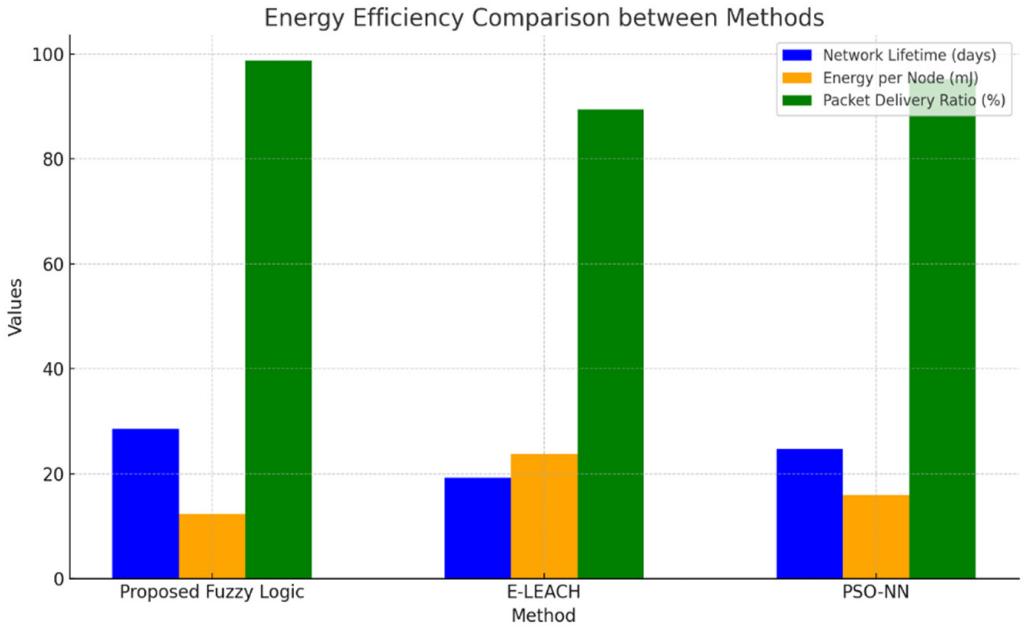

Fig. 5. Energy efficiency comparison between proposed and conventional methods

Using real-world datasets (e.g., CIC-IDS2017, Bot-IoT) ensures practical relevance. However, discrepancies in energy metrics between simulations (NS-3) and real

deployments (TinyOS) suggest environmental factors (e.g., radio interference) may slightly alter outcomes.

6 CONCLUSION AND FUTURE WORK

Wireless sensor networks face critical challenges in balancing robust cybersecurity with energy efficiency, particularly in adversarial environments. This paper proposed a DFLA to address these dual objectives through a decentralized architecture that integrates FIS for adaptive decision-making. For reducing centralized computation and facilitating node-level autonomy in decision-making, DFLA applies to resource-constrained environments. By fuzzifying metrics such as packet drop rate, residual energy, and signal strength deviation, DFLA achieves 99.87% detection accuracy for attacks like Blackhole and Flooding while reducing energy consumption by 48% compared to conventional protocols like E-LEACH. The distributed design minimizes communication overhead and computational complexity (15.2 KB/node memory footprint), enabling resource-constrained nodes to autonomously prioritize security or energy savings based on real-time risk assessments. Experimental validation using real-world datasets (WSN-DS, CIC-IDS2017) and testbeds (TinyOS, Edge-IIoTset) confirmed the algorithm's scalability, low latency (12.3 ms detection delay), and resilience to dynamic attack patterns. By harmonizing Dempster-Shafer theory for data fusion and metaheuristic optimization (Reptile Search Algorithm) for parameter tuning, DFLA bridges the gap between centralized ML models and rigid threshold-based methods, offering a practical solution for next-generation WSN deployments.

Future research will focus on enhancing DFLA's adaptability through federated learning to dynamically refine fuzzy rules and membership functions across distributed nodes, addressing dataset biases and environmental variability. Integrating lightweight reinforcement learning could further optimize the security-energy trade-off during prolonged attacks, mitigating the observed 12–15% energy spike in high-risk scenarios. Furthermore, while the system is effective on specific types of attacks, its resistance to zero-day or AI-based attacks remains to be thoroughly investigated. Future research will seek to resolve these issues by combining dynamic fuzzy rule learning, federated reinforcement learning, and scalable testing on ultra-large WSNs (e.g., 1,000+ nodes), further improving the model's robustness and real-world applicability. These advancements aim to solidify DFLA as a universal standard for secure, sustainable WSNs in evolving cyber-physical ecosystems.

7 REFERENCES

[1] M. H. Behiry and M. Aly, "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods," *J. Big Data*, vol. 11, no. 16, 2024. https://doi.org/10.1186/s40537-023-00870-w

[2] A. Verma, S. Kumar, P. R. Gautam, T. Rashid, and A. Kumar, "Fuzzy logic based effective clustering of homogeneous wireless sensor networks for mobile sink," *IEEE Sensors Journal*, vol. 20, no. 10, pp. 5615–5623, 2020. https://doi.org/10.1109/JSEN.2020.2969697

[3] G. S. Dhunna and I. Al-Anbagi, "A low power cyber-attack detection and isolation mechanism for wireless sensor network," in *Proc. IEEE 86th Vehicular Technology Conference (VTC-Fall)*, Toronto, ON, Canada, 2017, pp. 1–5. https://doi.org/10.1109/VTCFall.2017.8288185

[4] Z. Zhao, K. Xu, G. Hui, and L. Hu, "An energy-efficient clustering routing protocol for wireless sensor networks based on AGNES with balanced energy consumption optimization," *Sensors*, vol. 18, no. 11, p. 3938, 2018. https://doi.org/10.3390/s18113938

[5] O. I. Uzougbo, S. M. Ajibade, and F. Taiwo, "An overview of wireless sensor network security attacks: Mode of operation, severity and mitigation techniques," *arXiv preprint arXiv:2011.06779*, 2020. https://doi.org/10.48550/arXiv.2011.06779

[6] R. Verma and S. Bharti, "A survey of network attacks in wireless sensor networks," in *Information, Communication and Computing Technology*, *ICICCT 2020.* in Communications in Computer and Information Science, C. Badica, P. Liatsis, L. Kharb, and D. Chahal, Eds., Springer, Singapore, vol. 1170, 2020. https://doi.org/10.1007/978-981-15-9671-1_4

[7] O. Younis, and S. Fahmy, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," *IEEE Transactions on Mobile Computing*, vol. 3, no. 4, pp. 366–379, 2004. https://doi.org/10.1109/TMC.2004.41

[8] Y. Zhang, J. Wang, D. Han, H. Wu, and R. Zhou, "Fuzzy-logic based distributed energy-efficient clustering algorithm for wireless sensor networks," *Sensors*, vol. 17, no. 7, p. 1554, 2017. https://doi.org/10.3390/s17071554

[9] M. Gamal, N. E. Mekky, H. H. Soliman, and N. A. Hikal, "Enhancing the lifetime of wireless sensor networks using fuzzy logic LEACH technique-based particle swarm optimization," *IEEE Access*, vol. 10, pp. 36935–36948, 2022. https://doi.org/10.1109/ACCESS.2022.3163254

[10] M. Kumar, S. C. Sharma, and L. Arya, "Fuzzy based QoS analysis in wireless ad hoc network for DSR protocol," in *Proc. 2009 IEEE Int. Advance Computing Conference*, Patiala, India, 2009, pp. 1357–1361. https://doi.org/10.1109/IADCC.2009.4809214

[11] H. Hu, X. Fan, and C. Wang, "Efficient cluster-based routing protocol for wireless sensor networks by using collaborative-inspired Harris Hawk optimization and fuzzy logic," *PLoS ONE*, vol. 19, no. 4, p. e0301470, 2024. https://doi.org/10.1371/journal.pone.0301470

[12] Shilpi and A. Kumar, "Sensor node localization using nature-inspired algorithms with fuzzy logic in WSNs," *J. Supercomputing*, vol. 80, no. 19, pp. 26776–26804, 2024. https://doi.org/10.1007/s11227-024-06464-4

[13] L. Pirmez, F. C. Delicato, P. F. Pires, A. L. Mostardinha, and N. S. de Rezende, "Applying fuzzy logic for decision-making on wireless sensor networks," in *Proc. IEEE International Fuzzy Systems Conference*, London, UK, 2007, pp. 1–6. https://doi.org/10.1109/FUZZY.2007.4295421

[14] M. Abbas, D. Sarita, M. Alrasheedi, L. Arya, M. P. Singh, and K. Pandey, "Hybrid intuitionistic fuzzy entropy-SWARA-COPRAS method for multi-criteria sustainable biomass crop type selection," *Sustainability*, vol. 15, no. 10, p. 7765, 2007. https://doi.org/10.3390/su15107765

[15] L. Q. Thao *et al.*, "Optimizing tomato irrigation through deep learning-enabled wireless sensor networks with fuzzy logic," *Irrig. Sci.*, vol. 42, pp. 955–976, 2024. https://doi.org/10.1007/s00271-024-00949-z

[16] S. Nagaraj *et al.*, "Improved secure encryption with energy optimization using random permutation pseudo algorithm based on Internet of Thing in wireless sensor networks," *Energies*, vol. 16, no. 1, p. 8, 2023. https://doi.org/10.3390/en16010008

[17] A. D. Samala and M. Amanda, "Immersive Learning Experience Design (ILXD): Augmented reality mobile application for placing and interacting with 3D learning objects in engineering education," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 5, pp. 22–35, 2023. https://doi.org/10.3991/ijim.v17i05.37067

[18] S. Amri, F. Khelifi, A. Bradai, A. Rachedi, and M. L. Kaddachi, "A new fuzzy logic-based node localization mechanism for wireless sensor networks," *Future Generation Computer Systems*, vol. 93, pp. 799–813, 2019. https://doi.org/10.1016/j.future.2017.10.023

[19] I. Almomani, B. Al-Kasasbeh, and M. Al-Akhras, "WSN-DS: A dataset for intrusion detection systems in wireless sensor networks," *Journal of Sensors*, vol. 2016, no. 1, 2016. https://doi.org/10.1155/2016/4731953

[20] Zafar Iqbal Khan, Mohammad Mazhar Afzal, and Khurram Naim Shamsi, "A comprehensive study on CIC-IDS2017 dataset for intrusion detection systems," *International Research Journal on Advanced Engineering Hub (IRJAEH)*, vol. 2, no. 2, pp. 254–260, 2024. https://doi.org/10.47392/IRJAEH.2024.0041

[21] D. C. Muñoz and A.dC. Valiente, "A novel botnet attack detection for IoT networks based on communication graphs," *Cybersecurity*, vol. 6, no. 33, 2023. https://doi.org/10.1186/s42400-023-00169-6

[22] M. Dener, C. Okur, S. Al, and A. Orman, "WSN-BFSF: A new data set for attacks detection in wireless sensor networks," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 2109–2125, 2024. https://doi.org/10.1109/JIOT.2023.3292209

[23] Y. Liu, "GreenOrbs: Lessons learned from extremely large scale sensor network deployment," in *Database Systems for Adanced Applications*, *DASFAA 2011.* in Lecture Notes in Computer Science, J. Xu, G. Yu, S. Zhou, and R. Unland, Eds., vol. 6637, Springer, Berlin, Heidelberg, 2011. https://doi.org/10.1007/978-3-642-20244-5_38

[24] V. Shanmugam, R. Razavi-Far, and E. Hallaji, "Addressing class imbalance in intrusion detection: A comprehensive evaluation of machine learning approaches," *Electronics*, vol. 14, no. 1, p. 69, 2025. https://doi.org/10.3390/electronics14010069

[25] W. R. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks (LEACH)," in *Proceedings of the 33rd Annual Hawaii International Conference System Sciences*, vol. 2, 2000, p. 10. https://doi.org/10.1109/HICSS.2000.926982

[26] L. Abualigah, M. A. Elaziz, P. Sumari, Z. W. Geem, and A. H. Gandomi, "Reptile Search Algorithm (RSA): A nature-inspired meta-heuristic optimizer," *Expert Systems Applications*, vol. 191, p. 116158, 2022. https://doi.org/10.1016/j.eswa.2021.116158

[27] M. Ahmed, X. Huang, and D. Sharma, "Dempster-Shafer theory to identify insider attacker in wireless sensor network," in *Network and Parallel Computing (NPC 2012)*, in Lecture Notes in Computer Science, J. J. Park, A. Zomaya, S. S. Yeo, and S. Sahni, Eds., vol. 7513, Springer, Berlin, Heidelberg, 2012, pp. 94–100. https://doi.org/10.1007/978-3-642-35606-3_11

[28] R. Sethuraman *et al.*, "IT2FLS-RSA: A novel approach for QoS-driven routing and security enhancement in wireless sensor networks," *Int. J. Fuzzy Syst.*, 2025. https://doi.org/10.1007/s40815-025-01980-8

[29] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications: Centralized and federated learning," *IEEE Dataport*, 2022. https://doi.org/10.21227/mbc1-1h68

[30] A. K. Rai and A. K. Daniel, "FEEC: Fuzzy based energy efficient clustering protocol for WSN," *Int. J. Syst. Assur. Eng. Manag.*, vol. 14, pp. 297–307, 2023. https://doi.org/10.1007/s13198-022-01796-x

[31] A. D. Samala, N.-J. Howard, C. S. Criollo, R. D. A. Budiman, M. Hakiki, and Y. Hidayah, "What does an IMoART application look like? IMoART—An interactive mobile augmented reality application for support learning experiences in computer hardware," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 18, no. 13, pp. 148–165, 2024. https://doi.org/10.3991/ijim.v18i13.47565

[32] M. Hakiki *et al.*, "Enhancing practicality of web-based mobile learning in operating system course: A developmental study," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 17, no. 19, pp. 4–19, 2023. https://doi.org/10.3991/ijim.v17i19.42389

8 AUTHORS

Leena Arya is with the Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India (E-mail: leenaarya@kluniversity.in).

Gunjan Varshney is with the Department of Robotics and Artificial Intelligence, JSS University, Noida, Uttar Pradesh, India.

MPJ Santosh is with the Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India.

Venkata Rajani Katuri is with the Department of Computer Science Engineering, GITAM University, Hyderabad, Telangana, India.

Monika Bhatnagar is with the Department of Electronics and Communication Engineering, Galgotias College of Engineering & Technology, Greater Noida, Uttar Pradesh, India.

Ravi Rastogi is with the Department of CSE, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India.