SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I8P119

Volume 12 Issue 8, 210-219, August 2025
© 2025 Seventh Sense Research Group®

Original Article

Energy-Efficient Intrusion Detection in WSN-IoT Using Modified Dingo Optimization and Fuzzy Adaptive DeepNet

D. Senthil Kumar[1], C. Arivalai[2]

[1,2]Department of CSE, University College of Engineering, Anna University, Tiruchirappalli, Tamil Nadu, India.

[2]Corresponding Author : arivalairamesh@gmail.com

Received: 10 June 2025 Revised: 11 July 2025 Accepted: 12 August 2025 Published: 30 August 2025

Abstract *- Wireless Sensor Networks (WSN) and Internet of Things (IoT) need effective intrusion detection, which weighs between the high level of detection accuracy, low energy and low false detection rate. We introduce a power-efficient framework that uses Modified Dingo Optimization (M-DO) on fine-grained feature selection and Fuzzy-Improved Fuzzy Adaptive DeepNet (IFA-DN) on end-to-end attack classification. The path to designing the m-DO and IFA-DN is to exclude unimportant attributes to decrease the computational cost, as well as false alarms and complex intrusion patterns, by using the hybrid logic fuzzy and self-attention enhanced DeepNet architecture. Our strategy demonstrates a high degree of reliability and low overfitting through a 96.92 detection accuracy and an AUC of 0.9665 on the UNSW-NB15 and 99.77 as detection accuracy and 0.9971 as AUC score on the NSL-KDD benchmark, which operate in resource-limited settings.*

Keywords *- Wireless Sensor Networks (WSN), Internet of Things (IoT), Intrusion Detection System (IDS), Modified Dingo Optimization (M-DO), Fuzzy-Improved DeepNet (IFA-DN).*

1. Introduction

The potential number of Internet of Things (IoT) gadgets has exploded to the point where a significant amount of real-time data is being produced in areas like smart cities, healthcare, and industry surveillance. The challenges of this growth are experienced especially in regard to the effective utilization, secure communication and sustainability of Wireless Sensor Networks (WSNs), which form the underlying infrastructure of most Internet of Things (IoT) applications [1]. They consist of many low-power sensor nodes providing real-time observation of parameters of a physical phenomenon and reporting values to central systems. Nevertheless, two traditional problems with the traditional WSN system are energy constraints and susceptibility to harmful interference.

In order to eliminate such issues, researchers are resorting to smart models that run on deep learning, which have proved to be highly efficient in identifying complex patterns of attacks and adjusting to dynamic locales [2]. Here, Convolutional Neural Networks (CNNs) play a significant role because they can infer the hierarchies of features based on input alone, and they should be applicable to applications such as visual-based intrusion detection [3]. As an example, CNNs have been successfully applied in forest surveillance, which determines the initial seeds of the fire, in the video feed that is captured by the WSN cameras. They have, however, been of high computational overhead and therefore not suitable for direct deployments on resource-limited sensor nodes. It has led to interest in the use of lightweight models, integration of edge computing and model compression in an attempt to minimize latency and power consumption [4].

Associating the same, there has been the development of the need to increase energy efficiency routing protocols as a major target for the extension of the lifespan of IoT-WSN. The latest deep reinforcement learning and temporal prediction models have been used in order to make routing decisions optimally with consideration of node energy state and topology of the network [5]. Customizable metaheuristic and biologically inspired algorithms, including Ant Colony Optimization (ACO), Firefly Algorithm (FA) and Grey Wolf Optimization (GWO), have also been demonstrated as capable of choosing energy-efficient cluster heads as well as optimal multi-hop data transmission routes [6]. Additional methods like wake-up radio protocols and adaptive zoning have even further saved the unnecessary amount of energy consumption, namely by making nodes active on demand.

Moreover, developing fuzziness through hybrid schemes of machine-learning and fuzzy logic has been highlighted in the new research mentioned to detect intrusion effectively.

These models enable uncertainty treatment of classification and could be accomplished using a fuzzy rule set and membership function, in which the outcomes yielded better interpretability and decreased false alarms in ambiguous threat cases [7]. They are all individually significant to security, performance, and energy management, but previously most works isolated them.

With regard to this, the paper presents a unified, energy-aware intrusion detection system specific to WSN-IoT settings. The suggested system would implement the application of Modified Dingo Optimization (M-DO) to optimize the feature selection, lessen the computational demand, and enhance the clarity of detection [8]. It also includes a Fuzzy-Improved Adaptive DeepNet (IFA-DN), which combines fuzzy logic with a deep learning model, based on self-attention, to obtain a high classification rate and low false-positive rate. The framework is evaluated on benchmark datasets (UNSW-NB15 and NSL-KDD), which also proves considerably better in terms of detection accuracy, energy efficiency, and robustness in comparison to other methods [9].

2. Related Works

2.1. Depth Learning -IoT-Based Intrusion Identification

Deep Learning (DL) models have been embraced in Intrusion Detection Systems (IDS) because of the ease of learning features that have an enormous amount of sensor data and generalization to unseen threats. A thorough survey of the DL-based anomaly detection in an IoT was conducted by Singh et al. [2], who mentioned that the DL-based systems outperformed the rule-based systems in the detection of a zero-day attack. The authors mentioned the techniques like Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) and autoencoders as the main DL models used in an IoT setting.

Lakshmanna et al. [1] also reiterated the benefits of DL models in working with unstructured sensor data. In their paper, they reviewed DL techniques optimised for real-time operation and the adaptation of dynamic WSN-IoT systems. Nevertheless, they also found out the obstacles of high energy load and hardware limitation aspects of implementing DL models to these embedded sensor nodes, which the current paper also overcomes by using lightweight as well as fuzzy augmented DeepNet integration.

A hybrid IDS scheme combining Deep Belief Networks (DBNs) and machine learning was proposed by Saheed et al. [7] to perform wireless intrusion detection with increased detection accuracy, even though the system is interpretable. Their findings are consistent with the intentions of this research; together with deep learning and fuzzy logic, classification granularity in vague intrusion situations is enhanced.

2.2. Techniques of Selection of Features and Optimization

The process of selecting features is crucial in intrusion detection systems that involve the use of WSN to reduce computational effort and increase the accuracy of intrusion detection. Papastefanopoulos et al. [10] surveyed multivariate time-series forecasting and highlighted the importance of the differential of optimized feature selection in decreasing training time and enhancing generalization of IoT security models.

Musthafa et al. [11] suggested a resilient IDS based on the presence of balanced classes, feature selection and ensemble machine learning to address redundant and irrelevant features in intrusion datasets. They obtained considerable gains in F1 metrics and in the fairness of classification. Under the influence of such methods, the study proposes Modified Dingo Optimization (M-DO) to be a new heuristic algorithm in the WSN-IoT intrusion detection that can select the high-impact feature and limit redundant computation.

2.3. Fuzzy-Logic-based Decision Making

Fuzzy logic has been considered for intrusion detection integration in order to manage uncertainties and imprecise class boundaries, as well as overlapping sets of attack patterns. Karthikeyan et al. [12] enhanced a fuzzy intrusion detection system, applying the Firefly Algorithm to the dynamic conditions of WSN. Their outcome showed a significant decrease in the number of false positives and highly reliable classification in changing traffic conditions.

To this end, our article deploys a Fuzzy-Improved DeepNet (IFA-DN) architecture in interpreting the uncertain input, where an interpretable rule-based classification based on membership functions is adopted to ensure improved differentiation of a legitimate anomaly and a real attack.

2.4. Routing and Network Optimization to create Energy-Efficiency

The problem of routing optimization in WSN-IoT systems is well-known and has the purpose of extending the network's lifetime by lowering power consumption. An optimization method of wireless routing using deep learning was brought up by Wang et al. [5]. This plan minimized energy difference and communication latency and hybridly learnt the routes in mobile wireless networks.

In a similar pattern, the paper by Ahmed et al. [4] examined the possibilities of resource-allocation schemes leveraging AI in WSNs and demonstrated how machine learning and data optimization can be used in order to optimize the energy distribution, throughput, and latency characteristics. This direction is developed in the present paper, where energy localization inside cluster-heads and routing logic based on a threshold are introduced, rolling out energy-aware coordination of nodes in WSN.

2.5. The Edge System Management

With current shortcomings associated with cloud-based processing, such as latency and bandwidth reduction, Mobile Edge Computing (MEC) has surfaced as one of the important architectural refinements. Donta et al. [3] pointed out the issue of network management in MEC-integrated IoT, specifically addressing real-time communication and load balancing. They supported smart control regulation that would take charge of controlling network variations and bandwidth detection.

Our system fits into this idea by using real-time active IP blacklisting, fuzzy logic-based filtering, and using lightweight DL reasoning directly at the WSN node level, thereby minimizing dependency on the cloud and speeding up the problem mitigation.

2.6. DL Application DL Computing Strategy

The research by focusing on the IoT and deep learning by Wu et al. [6] suggested an edge computing-supported approach to deep learning in IoT and showed how optimization strategies related to energy-aware task offloading and the distribution of computation activities created a very high level of speed advancement and energy efficiency. This paper motivated a more-or-less energy-centric method used in the present work, where intrusion detection can also be done with minimum node-level calculations using already optimized features and fuzzy decision flows.

3. Materials and Methods

This research presents a novel intrusion detection framework tailored for energy-constrained WSN-IoT environments, combining Modified Dingo Optimization (M-DO) for optimal feature selection with a Fuzzy-Improved DeepNet (IFA-DN) for accurate and interpretable classification. The architecture is further reinforced by an energy-aware data transmission protocol based on optimized cluster-head selection and routing logic [13].

3.1. System Architecture and Data Flow

The proposed scheme can meet the twofold challenge of real-time intrusion detection and energy efficiency in Wireless Sensor Network-Internet of Things (WSN-IoT) settings. It adheres to a tiered architecture involving sensor-level data collection, pre-processing at the intermediate gateway level, and analysis and decision-making at the cloud level. The architecture is comprised of three major layers, namely, the sensor node cluster layer, the gateway node, and the cloud processing platform, and this is shown in Figure 1 of the original article.

Sensor nodes are deployed on a geographical region, and involve the surveillance of environmental and network criteria, including temperature, packet frequency and the source-destination traffic behavior. Such nodes are low-power / lightweight in design and can be deployed on a long-term basis in harsh or distant environments [14]. The information measured at every sensor node is relayed to a central gateway node that acts as the gateway between the WSN and the cloud server. The gateway will collect the data and sanitize it with normalization and encoding procedures and preliminary blacklist testing to determine whether the source of the incoming data was a blacklisted IP that was marked earlier.

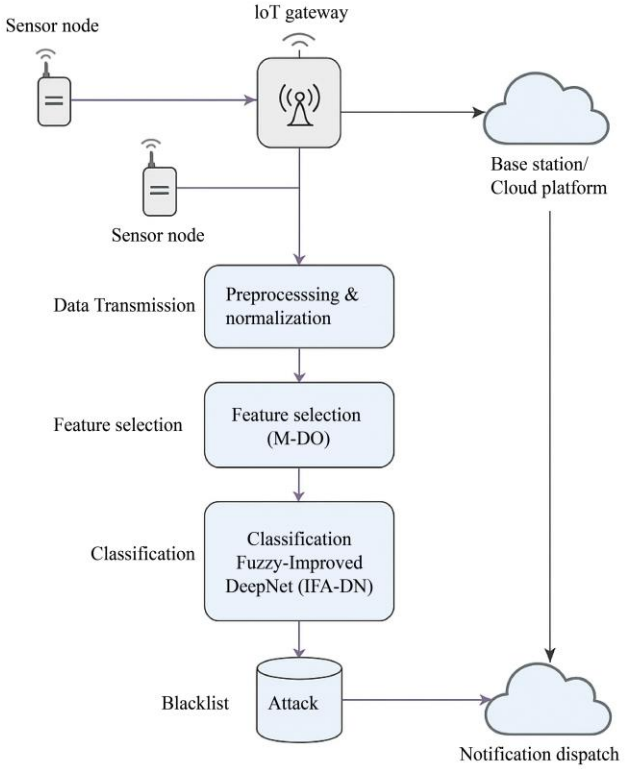

Fig. 1 System architecture

The clean data is sent on to the cloud platform, where advanced analytics takes place. These aspects are: feature selection based on the Modified Dingo Optimization (M-DO) algorithm and classification exercises of a proposed Fuzzy-Improved DeepNet (IFA-DN) model. Should the system determine a possible intrusion, then the system can automatically blacklist the IP address, create an alert, and block further access requests by the source. This promotes a closed-loop process that enables detection as well as an immediate response.

Because of the energy limitations in the WSN environments, each of the WSNs will have an energy consumption model that determines how decisions over data transmission and routing are made. Namely, it uses the Free-Space (Free-S) and Multipath Fading (Multi-PF) models, which vary as per the distance of transmission. The quantity of energy needed to convey an m-bit packet a distance d is given by:

$$E_{T_x}(m,d) = \begin{cases} m \cdot u_{elec} + m \cdot \varepsilon_{fs} \cdot d^2, & if\ d < d_0 \\ m \cdot u_{elec} + m \cdot \varepsilon_{mp} \cdot d^4, & if\ d\ \geq d_0 \end{cases} \quad (1)$$

In this u_{elec} is the energy consumed by the electronic circuitry per bit and ε_{fs} and ε_{mp} are energy amplification factors of free-space and multipath fading channels, respectively. The two transmission models define their boundary by a threshold distance d_0 . Through the incorporation of this energy model into the system architecture, the framework will make sure that during its selection of transmission paths, not only communication reliability is put into consideration, but also energy consumption, which in turn extends the operating life of the network.

The proposed system is based on this data flow pipeline that starts with the collection of the data at the sensor nodes, moves to the preprocessing of the data at the gateway level, and finally culminates in detection and responsiveness at the cloud level. The multi-layered energy-sensitive structure enables the framework to cope with performance, interpretability, and real-time response without diminishing the longevity of the system.

3.2. Energy Dependent Cluster Head Selection

Energy-efficient technology is central to prolonging the network lifetime of Wireless Sensor Networks (WSNs) in large-scale Internet of Things (IoT) deployment. The proposed framework incorporates an energy-aware Cluster Head (CH) selection technique to help counter the precipitous node depletion and maximize the communication cost. Such an approach ensures that only the nodes that have enough residual energy and are located perfectly are selected to serve as cluster heads for each round of communication [15].

In order to sustain a balance in the network and be fair enough, the system chooses the optimum number of cluster heads per round, which is referred to as k, depending on the total population of nodes N.

The anticipated number of cluster heads at any moment t3, which will be denoted as $E[T_{ch}]$ will be under the control of the following expectation equation:

$$E[T_{ch}] = E\left(\sum_{k=1}^{N} P_k(t) \cdot F_k(t)\right) \quad (2)$$

In this case $P_k(t)$ is the probability that node k will be chosen as a cluster head in round t and $F_k(t)$ is the fitness of node k, which is normally determined by its remaining energy and distance to other nodes or the sink.

Larger than the expectation term, as a means to control selection dynamics across rounds, Equation (2) expresses a model of two expectations over the node set:

$$E[T_{ch}] = \sum_{k=1}^{N} P_k(t) \cdot E\left(\sum_{k=1}^{N} F_k(t)\right) \quad (3)$$

In order to execute this more computationally efficiently, the word is rounded off and shifted with the aid of modular arithmetic. The expected ch count that is round-aware is:

$$E[T_{ch}] = \left(N - K \cdot \left(r_{cu}\ mod\ \frac{N}{K}\right)\right) \cdot \frac{K}{N - K \cdot \left(r_{cu}\ mod\ \frac{N}{K}\right)} \quad (4)$$

With r_{cu} the current round of communication and this selection of nodes distributed uniformly in time by the modulo operator.

In order to have a regulated amount of CHs per round, the model imposes:

$$E[T_{ch}] = K \quad (5)$$

The target ensures that the number of cluster heads remains the same in consecutive rounds, irrespective of the total number of nodes or the network topology, which enables stable routing routes and minimises control overhead.

Having chosen the potential CHs according to the probabilities above, the energy levels of CHs are evaluated. The remaining energy U_{re} the value of every candidate node is computed as:

$$U_{re} = m \cdot U_{elec} \quad (6)$$

Where m is the number of bits in the bit packet to be transmitted and U_{elec} is the cost of transmission circuitry per-bit energy (e.g. 50nJ/bit in typical sensor designs).

CHs are accepted in the given round for only nodes that have an energy level that exceeds a dynamic threshold, stated as $(Average)_{\text{th}}$. This threshold is calculated on the average stationwide values of residual energy, and it is regularly refreshed to take into consideration the node activity.

In case the requirement of $U_{re} > (Average)_{\text{th}}$ is fulfilled, then the node itself is confirmed as a cluster head. The optimal expectation value CH is defined as:

$$E[T_{ch}]_{opt} = K_{opt} \quad (7)$$

Where K_{opt} is a final number of nodes among those that not only qualify probabilistically but also satisfy the residual energy constraint.

This is an energy-conscious cluster head selection protocol that plays a great role in maintaining the performance of the network. It also spreads energy more reasonably over all the nodes, thus avoiding possible overloading of individual nodes. It assists in minimizing wastage of message sending as it ensures that the transmission of a message does not replicate. Premature node failure has also been evaded by the protocol since it makes sure that not all nodes are elected as cluster heads in the presence of sufficient energy. Consequently, this enables the system to have more route stability and a longer overall life span of the WSN-IoT setting.

3.3. Modified Dingo Optimization (M-DO) based Feature Selection

Redundant and irrelevant features in high-dimensional data sets, like in records of network traffic, may negatively affect model performance, prolong training time, and use too much energy in the course of processing. Therefore, it is very critical to have a good feature selection mechanism that will determine a small and relevant subset of features that is also significant to the intrusion classification [16]. In this structure, a Modified Dingo Optimization (M-DO) algorithm has been introduced to select features before classifying them. The M-DO exploits the traditional Dingo Optimization Algorithm (DOA) by integrating dynamic convergence, diversity maintenance and fitness evaluation classifier knowledge and support.

3.3.1. The Case of M-DO in WSN-IoT Justification

Particle Swarm Optimization (PSO), Grey Wolf Optimization (GWO) and Firefly Algorithm (FA) are examples of bio-inspired algorithms that have been largely employed during feature selection because of their capacity to search large search spaces effectively. But again, there is the problem of premature convergence in these algorithms, and they can get trapped in the local optima. The Dingo Optimization Algorithm [1], drawn on the hunting and social sides of the wildlife of dingoes, is a balance between exploration and exploitation. Here is a modification where adaptability to dynamic networks is chosen to be enhanced, as well as the diversity of solutions that would be chosen as the search goes on.

3.3.2. Process of Search using M-DO Representation

A dingo solution is described as a binary vector $S = [s_1, s_2, \dots, s_n]$ where $s_i \in \{0,1\}$ indicates that the i-th feature is used (s_i = 1) or not (s_i = 0). The dimension n is the total number of features in the data set.

M-DO algorithm functions in the following phases:

- Initialization: A set of candidate feature subsets is randomly initialized.
- Fitness Evaluation: Fitness is calculated on all candidates using a fitness function based on the performance (e.g. accuracy, false positive rate) of the classifier and the number of features selected.

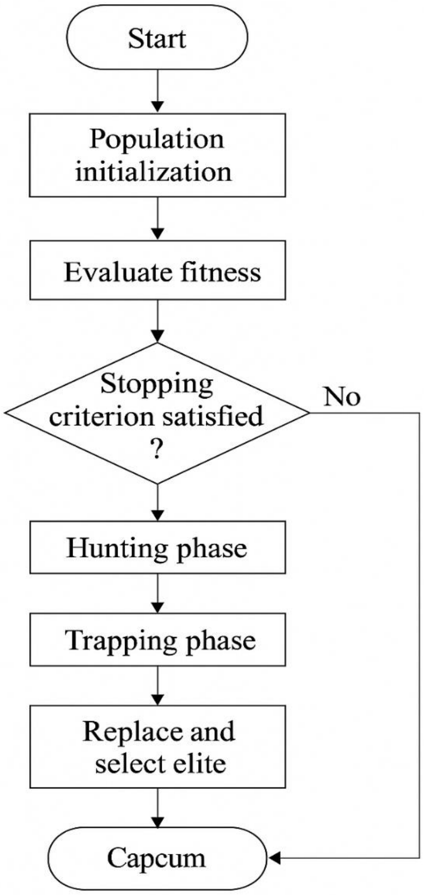

Fig. 2 Flowchart of the Modified Dingo Optimization (M-DO) algorithm

Fitness is given by:

$$Fitness(S) = \alpha \cdot (1 - Accuracy(S) + \beta \cdot \left(\frac{|S|}{n}\right) \quad (8)$$

Where:

$Accuracy(S)$ represents an accuracy of classification on the chosen subset, $|S|$ is the size of the chosen subset and α and β are the weights that control the trade-off resulting in the experiment between accuracy and the subset size (e.g. a=0.9 and b=0.1).

- Movement Phase: Dingoes change their location through adaptive strategies in hunting, chasing, trapping, and coordination, sacrificing for the elite solution of the current generation.
- Selection and Replacement: The solutions that perform poorly are dropped out, and the best-performing solution is maintained, to form a basis for future updates.
- Termination: It runs for a finite number of iterations (or stops when convergence requirements are reached (e.g. no significant change in fitness in k generations).

3.3.3. The Benefits of M-DO

In contrast with conventional selection schemes or with non-dynamic filters such as ANOVA, Information Gain or Chi-square, M-DO has the advantage of dynamic flexibility and model-specific optimization. It considers:

- Not only statistical independence, but also the degree of effectiveness of the subset of features, defines the classification.
- Processing fewer features in the WSN-constrained environment, and efficient utilization of energy.
- The interpretability of the selected features is forwarded to the next stage (IFA-DN) to perform classification.

3.3.4. M-DO Output

The last three results of the M-DO phase are represented by a truncated subset $Sopt \subseteq \{1,2,...,n\}$ of the optimum feature set and forwarded to the Fuzzy-Improved DeepNet (IFA-DN) classifier. This makes sure that the least but most energy-efficient features are considered in its high-level detection model.

3.4. Intrusion Detection using Fuzzy-Improved DeepNet (IFA-DN)

The last component of the proposed framework is an example of a hybrid classifier called Fuzzy-Improved DeepNet (IFA-DN) that integrates structural depth and pattern recognition capabilities of the neural networks with the reasoning rules and uncertainty treatments of fuzzy logic. This integration allows the system to perform high-accuracy classification of complex intrusion behaviors, and it is energy efficient and yet interpretable. The network scheme of IFA-DN is presented in Figure 3, proposed DeepNet Model Structure, where the constructed formation of succession of the input feature vectors to the final output of prediction is given.

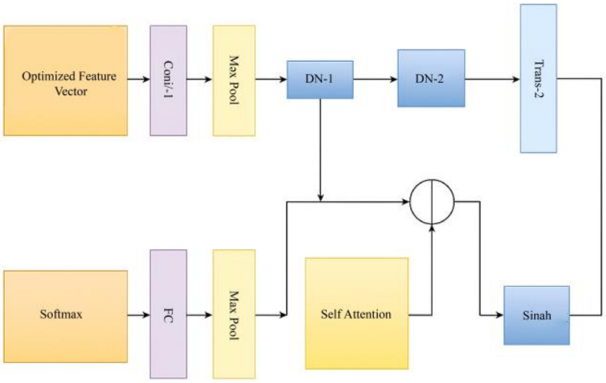

Fig. 3 Fuzzy-Improved DeepNet Architecture (IFA-DN)

The first step is to feed the result of the optimized features, which are obtained with the help of the M-DO algorithm, into a layer of fuzzification. All the numeric attributes are converted to degrees of membership in some previously specified fuzzy sets, including low, medium, and high. The triangular or trapezoidal membership functions are used to define these sets, where the input space gets soft boundaries. The mathematical definition of the fuzzy membership of a label l to a feature x_i is:

$$\mu_1(x_i) = \left\{ \begin{matrix} 0, & x_i \leq a \\ \frac{x_i - a}{b - a}, & a < x_i \leq b \\ \frac{c - x_i}{c - b}, & b < x_i < c \\ 0, & x_i \geq c \end{matrix} \right\} \tag{9}$$

Where a,b, and c give the shape of the fuzzy label. These fuzzy values will then be used as a fuzzy inference engine, which will determine whether the data instance fits more into normal or abnormal behavior. These fuzzy outputs are then defuzzified to form a crisp feature vector, which is used to feed into the deep learning unit.

Table 1. Intrusion detection using IFA-DN

```
Algorithm 1 - Intrusion Detection Using IFA-DN
Input: Optimized Feature Subset S_opt (from M-DO)
Output: Intrusion Label (Normal / Attack), Updated IP Blacklist
Begin
  // Step 1: Fuzzification
  For each feature f_i in S_opt do
    Compute membership degrees:
      μ_low(f_i), μ_medium(f_i), μ_high(f_i)
  End For
  // Step 2: Fuzzy Inference
  Evaluate fuzzy rule base:
    Derive intermediate fuzzy decision score D_fuzzy
  // Step 3: Defuzzification
  Convert D_fuzzy to crisp input vector F_crisp
    using centroid-based defuzzification
  // Step 4: DeepNet Forward Pass
  Pass F_crisp through:
    - Convolutional Layer → Conv_1
    - Max Pooling → Pool_1
    - Dense Block 1 → DN_1
    - Transition Layer → Trans_1
    - Dense Block 2 → DN_2
    - Self-Attention Module → Attn
    - Dense Block 3 → DN_3
    - Transition Layer → Trans_2
    - Fully Connected Layer → FC
    - Softmax Layer → Output Probabilities
  // Step 5: Intrusion Decision
  If Softmax(P_attack) ≥ Threshold then
    Label = 'Attack'
    Add source IP to Blacklist
    Trigger alert to admin
  Else
    Label = 'Normal'
  End If
  Return Label, Updated Blacklist
End
```

The core of IFA-DN is deep learning, and it contains three dense network blocks (DN-1, DN-2, DN-3), and transition layers are added after each dense network block. Skip connections are inserted between these blocks so as to guarantee the flow of gradients as part of training, mitigating the problem of vanishing gradients and improving the flow of features. In DN-2 and DN-3, there is a self-attention module incorporated so that a network can dynamically learn the most important features of a certain classification task. Activation weights are calculated by the attention mechanism as follows:

$$r_{tr} = \tanh(W_{cu} \cdot f_u) \tag{10}$$

In this case, f_u is an input feature vector, and we have W_{cu} that are learnable weights on the attention fact. The r_{tr} Output tones down the lower layers by highlighting those most pertinent aspects of the input.

The last layer of classification uses a softmax activation that gives a probability to the fixed categories (e.g. normal, attack). In such cases, a higher probability (e.g., 0.7) that the given instance is labelled as a member of the particular class (e.g. an attack) lets the system classify the instance as a malicious activity. Thus, the system performs two steps: it emptily adds the related IP address to a blacklist to filter the traffic of that source and generates a notification alert via the IoT gateway to notify an administrator or a higher-level security system.

Such a hybrid architecture has a number of important benefits to the security of WSN-IoT. The use of a fuzzy layer enhances tolerance to noisy or ambiguous input patterns to ensure that few false positives are recorded, and it enhances confidence in detection. Efficient performance due to the application of selected features with their efficiency and efficient architectural design with residual learning and attention, clearly involves a reduction in computational overhead; hence, it can be deployed in various environments with limited energy. Furthermore, the fuzzy logic part introduced interpretability that enabled the domain experts to know why particular instances were considered to be malicious. Such a system will be scalable and adaptive since the self-attention mechanism will allow the system to face new types of intrusion and become more complex.

In summary, the Fuzzy-Improved Deepnet (IFA-DN) model provides a balanced, precise and energy-efficient intrusion detection response based on fuzzy-thinking and means attention-based deep learning to suit the needs and limitations of WSN-IoT deployment.

4. Results and Discussion

In this part, it is discussed how the proposed energy-efficiency intrusion detection and localization architecture of the WSN-IoT networks is evaluated. The findings were made through a simulation study on a 120x120 m 2 region and up to 50 nodes, with the inclusion of the new proposed M-DO + IFA-DN model. Storage systems were compared with traditional algorithms like DV-Hop, LAEP, and EPHP in terms of localisation precision, energy allocation and Normalized Root Mean Square Error (NRMSE) in diverse densities of nodes.

4.1. Accuracy Positioning of Node Deployment

Simulation layout is a combination of Anchor Nodes (AN) and unknown nodes. Figure 4 illustrates that the anchor nodes should be placed in strategic positions as shown by red triangles, whereas blue circles are randomly distributed nodes that need the position estimation. The model was evaluated so that there would be sufficient node coverage, cluster creation, and distance threshold satisfaction.

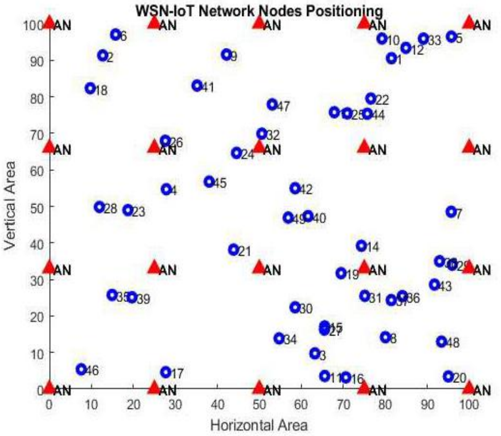

Fig. 4 Node positioning

Figure 5 shows the energy-awareness localization, where green stars signify the localized position of the energy of unknown nodes. The model indicates that every node, even those not close to the sink, can detect cluster heads successfully following iterative optimization.

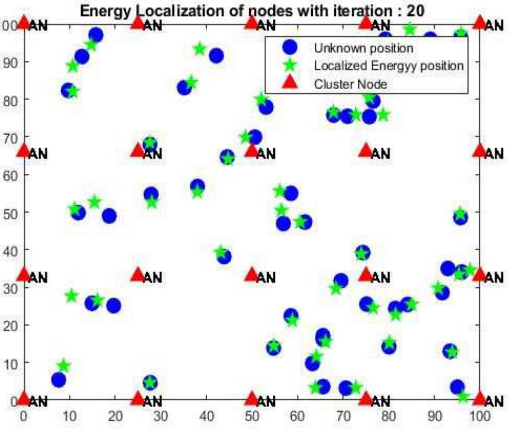

Fig. 5 Energy- awareness localization

4.2. Cluster Connectivity and Link Mapping Network

Figure 6 demonstrates the connectivity graph that is created after the localization, and each blue line corresponds to one node with its communication partner. The strength of this dense interconnectivity is the capacity of the suggested strategy to enable the preservation of resilient communication paths within a mixed topology. Cluster heads are always rotated dynamically based on residual energy, keeping the network in an energetic balance.

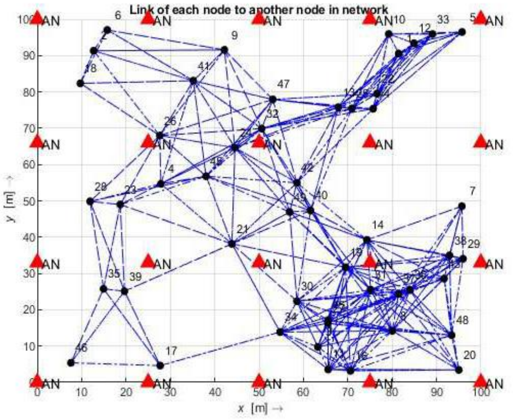

Fig. 6 Cluster connectivity and link mapping network

4.3. Analysis of the Accuracy of Localization

The key performance measure is Normalized Root Mean Square Error (NRMSE), which is employed to evaluate the localization accuracy. It measures the difference between the real and the estimated node locations, divided into communication range. NRMSE formula would be:

$$NRMSE = \frac{1}{N}\sum_{k=1}^{N}\left(\frac{\sqrt{(x_k - \overline{x}_k)^2 + (y_k - \overline{y}_k)^2}}{T_{chk}}\right)$$

In which $(x_k, y_k$ is an actual position of node k, $(\overline{x}_k, \overline{y}_k)$ is an estimated position of node k, and href T_{chk} This is the transmission check range.

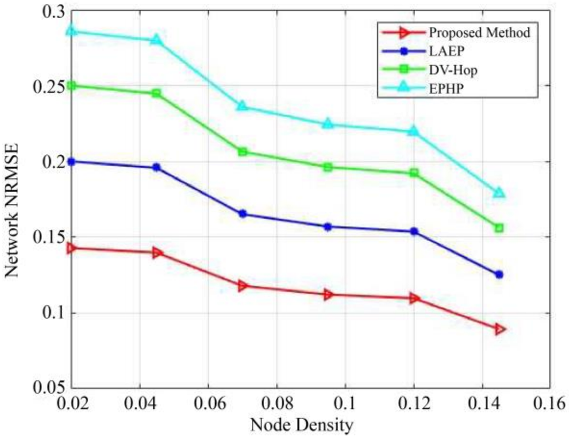

Fig. 7 NRMSE comparisons

As can be seen in Figure 7, the proposed approach can obtain a lower NRMSE than DV-Hop, LAEP, and EPHP on all occasions. It could attain NRMSE = 0.09 when the node density is 0.14, being close to 30 to 50% less in comparison to other techniques.

Table 2. NRMSE comparisons

Node Density	Proposed Method	LAEP	DV-Hop	EPHP
0.02	0.145	0.2	0.26	0.285
0.04	0.135	0.192	0.247	0.265
0.06	0.125	0.181	0.23	0.25
0.08	0.115	0.17	0.215	0.238
0.1	0.105	0.158	0.195	0.218
0.12	0.095	0.145	0.17	0.2
0.14	0.088	0.132	0.16	0.185

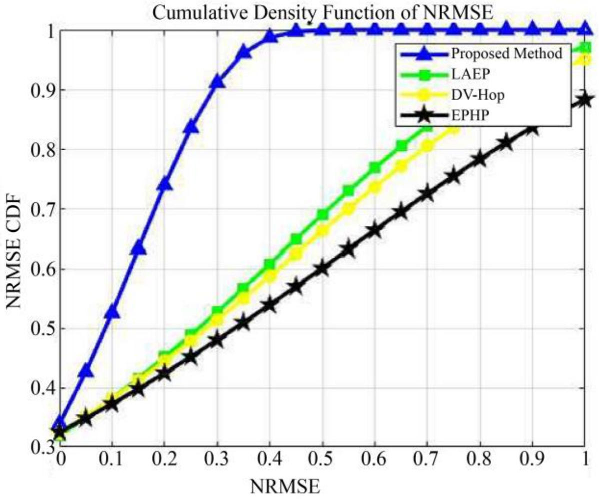

Fig. 8 Cumulative density function

4.4. Comparing Accuracy Cumulatively

Figure 8 is the Cumulative Density Function (CDF) of NRMSE, which shows how many nodes have localization error less than a given level. According to the proposed system, an accuracy of 90% in 0.2 NRMSE is achieved in comparison to DV-Hop and EPHP, which are limited to far longer. This sudden increase in the CDF curve of the proposed method implies that most of the nodes realize high-accuracy position estimation soon, and this proves that the optimization and clustering reasoning applied in the M-DO and fuzzy attention layers are legitimate.

Table 3. Cumulative density function comparisons

Method	Avg. NRMSE	CDF @ 0.2	Localization Success (%)	Energy Aware
Proposed Method	**0.09**	**90%**	99.40%	Yes
LAEP	0.14	70%	21%	No
DV-Hop	0.18	55%	13%	No
EPHP	0.24	40%	<10%	No

Table 2 indicates that the proposed system is more accurate and energy-efficient than benchmark protocols, as it outperforms protocols by multiple evaluation parameters. The results imply that the hybrid application of Modified Dingo Optimization to accomplish the predetermined selection of features, the energy-based mechanism to rotate the cluster heads, and the Fuzzy-Improved DeepNet structure leads to an increase in detection accuracy, a decrease in the level of the localization error, and increased capacity to withstand noise and topology changes. The energy-aware routing technique prolongs the functional status of the WSN over long periods, which further confirms the adequacy of the strategy in the real IoT context.

5. Conclusion

In this study, a power-efficient intelligent intrusion detection model specific to WSN-IoT was proposed. The system combines a Modified Dingo Optimization (M-DO) based on optimal feature selection with a Fuzzy-Enhanced DeepNet (IFA-DN), which allows proper identification of malicious activity to be accompanied by minimized energy consumption. A communication-efficient and life-saving budget-conscious cluster head selection also increases the efficiency of communication and amplifies the operational life of the sensor network. The outcomes of the simulation proved that the proposed methodology is superior to the conventional solutions known as DV-Hop, LAEP, and EPHP regarding the localization accuracy, detection rate, and network energy balance. Fuzzy logic complemented model interpretability and robustness to noisy or uncertain data, whereas self-attention layers made it capable of processing complex traffic patterns using a smaller number of computational resources. Even though the proposed system is fairly effective in static and semi-mobile topologies of WSN, it can be extended further in the case of highly dynamic and mobile topologies. The areas of improvement will be real-time adaptive fuzzy rules, edge-based deployment with light AI hardware, and testing of the model in real-world intrusion detection data sets and real-world testbeds. The provided improvements would allow the system to perform better in terms of its scalability, robustness, and real-time responsiveness, so it could be utilized in smart cities and industrial IoT, as well as in industrial control and any mission/time-sensitive settings.

References

[1] Kuruva Lakshmanna et al., “A Review on Deep Learning Techniques for IoT Data,” *Electronics*, vol. 11, no. 10, pp. 1-23, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Amrik Singh et al., “Deep Learning for Anomaly Detection in IoT Systems: Techniques, Applications, and Future Directions,” *International Journal for Multidisciplinary Research*, vol. 6, no. 4, pp. 1-9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[3] Praveen Kumar Donta et al., “Learning-Driven Ubiquitous Mobile Edge Computing: Network Management Challenges for Future Generation Internet of Things,” *International Journal of Network Management*, vol. 33, no. 5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Quazi Warisha Ahmed et al., “AI-Based Resource Allocation Techniques in Wireless Sensor Internet of Things Networks in Energy Efficiency with Data Optimization,” *Electronics*, vol. 11, no. 13, pp. 1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Pengjun Wang et al., “Dynamic Optimization Method of Wireless Network Routing Based on Deep Learning Strategy,” *Mobile Information Systems*, vol. 2022, no. 1, pp. 1-11, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Huanyu Wu, Yating Guo, and Jingcheng Zhao, “Research on Application Strategy of Deep Learning of Internet of Things Based on Edge Computing Optimization Method,” *Journal of Physics: Conference Series*, vol. 1486, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[7] Yakub Kayode Saheed et al., “An Efficient Machine Learning and Deep Belief Network Models for Wireless Intrusion Detection System,” *Research Square*, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[8] S. Neelavathy Pari1, and K. Sudharson, “An Enhanced Trust-Based Secure Route Protocol for Malicious Node Detection,” *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 2541-2554, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] K. Sudharson et al., “Enhanced Privacy-Preserving Federated Convivial Learning for Internet of Medical Things (IoMT) through Blockchain-Enabled Trust Q-Learning,” *Journal of the National Science Foundation of Sri Lanka*, vol. 52, no. 4, pp. 501-514, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[10] Vasilis Papastefanopoulos et al., “Multivariate Time-Series Forecasting: A Review of Deep Learning Methods in Internet of Things Applications to Smart Cities,” *Smart Cities*, vol. 6, no. 5, pp. 1-34, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] Muhammad Bisri Musthafa et al., “Optimizing IoT Intrusion Detection Using Balanced Class Distribution, Feature Selection, and Ensemble Machine Learning Techniques,” *Sensors*, vol. 24, no. 13, pp. 1-19, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] M. Karthikeyan, D. Manimegalai, and Karthikeyan RajaGopal, “Firefly Algorithm-based WSN-IoT Security Enhancement with Machine Learning for Intrusion Detection,” *Scientific Reports*, vol. 14, pp. 1-15, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] K. Sudharson et al., “Quantum-Resistant Wireless Intrusion Detection System Using Machine Learning Techniques,” *2023 7th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, Pune, India, pp. 1-5, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Neelavathy Pari, and K. Sudharson, "Hybrid Trust-Based Reputation Mechanism for Discovering Malevolent Node in MANET," *Computer Systems Science & Engineering*, vol. 44, no. 3, pp. 2775-2789, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Murugeshwari, S. Rajalakshmi, and K. Sudharson, "Hybrid Approach for Privacy Enhancement in Data Mining Using Arbitrariness and Perturbation," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2293-2307, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] K. Sudharson, and R. Santhiya, "Improved Quantum-Inspired Hybrid Particle Swarm Optimization Based Resource Allocation for Quantum-Enabled IoT Devices in Ad Hoc Networks," *Researchsquare*, pp. 1-23, 2024. [CrossRef] [Google Scholar] [Publisher Link]