The Bioscan
AN INTERNATIONAL QUARTERLY JOURNAL OF LIFE SCIENCES
20(4): 44-54, 2025 www.thebioscan.com

A Novel Routing Protocol for Data Transmission in WSNs with Security enhancement and Extended Lifetime using A Hybrid Deep Learning and Optimization Approach

S. Vishalini[1*], A. Kavitha[2]

[1*]Department of Computer Science, Kongunadu Arts and Science College, Coimbatore-641029, TN, India
vishaliniramesh.3394@gmail.com
[2]Department of Computer Science, Kongunadu Arts and Science College, Coimbatore-641029, TN, India
kavithaathinarayanan@gmail.com

DOI: 10.63001/tbs.2025.v20.i04.pp44-54

KEYWORDS:
Wireless sensor networks (WSNs), Routing Protocol (RP), Data Transmission (DT), Security, deep learning, Cluster Heads, GNN, Reinforcement Learning (RL), dynamic routing optimization

Received on:

31-08-2025

Accepted on:

01-10-2025

Published on:

03-11-2025

ABSTRACT

In many applications like smart infrastructure, healthcare facilities, army surveillance, and environmental monitoring, the Wireless Sensor Network (WSN) is crucial. The effectiveness of the WSN is limited by the following factors: low power sources, poor routing, security susceptibilities, prolonged delay, and the crucial demands in preserving Quality of Service (QoS). Optimizing QoS and robustness are the main emphasis of conventional methods. These conventional methods fail to offer this solution. This comprehensive solution is an integrated strategy that tackles a challenging issue by simultaneously considering several significant variables. For resolving these issues, a novel routing protocol (RP) is suggested in this study. Implementation of this suggested method may support in improving data transmission (DT), security, and the lifetime of WSN. The process begins with data pre-processing method. For effectively training deep learning (DL) module, this suggested method utilizes Robust Scaling approach. The cluster head (CH) is selected by utilizing hybrid Particle Swarm Optimization-Fuzzy C-Means (PSO-FCM) clustering technique, and this may result in optimizing the cluster formation process of the network. After the clustering method, route discovery method is implemented. The Graph neural network (GNN) and symmetric butterfly optimization algorithm (SBOA) are integrated in this route discovery method. This GNN facilitate precise data classification. The dynamic routing optimization is done via SBOA. For securing networks from these cyber threats, blockchain (BC)-based authentication is used. Thus, overall security of the system is improved. This hybrid method promotes in data management, energy efficiency (EE), and network security. The suggested strategy considerably increases the operational lifespan of WSNs when compared to current methods, and it was demonstrated by simulation outcomes.

INTRODUCTION

Hundreds of sensors are dispersed throughout a vast area in WSNs. WSN distributes and effectively processes the collected data and managing the environment [1,2]. Biological, chemical, and nuclear radiation detection, environmental monitoring and protection, agricultural monitoring, industrial product control, and military operations (to locate and organise troops in hostile territory) are only a few of the various applications for these networks [3]. Furthermore, the protection of commercial and cultural landmarks, smart cities, smart transportation, and smart homes all make use of WSNs [4,5].

The batteries that power the nodes in WSNs are rarely changed or refreshed. When detecting, processing, and transmitting environmental data, these nodes need a lot of energy. DT uses more energy than sensing and data processing [6]. In WSN, energy consumption (EC) management is therefore crucial. Clustering is one of the efficient ways to accomplish this objective. Both EE and transmission bandwidth are maintained in a clustered topology [7]. Sensor nodes (SN) in this topology have different tasks and the network is split up into various clusters. Choosing CH is a crucial risk in this situation.

To resolve this limitations, it is imperative to look into novel approaches like meta-heuristic algorithms (MHA). Intra-cluster and inter-cluster

communication are the two types of communications defined by cluster-based (CB) RP. These techniques increase network lifetime (NL) and are scalable and effective in terms of EC. Cluster-based routing for WSNs is the topic of holistic research in recent years. Then, WSNs have many limitations compared to traditional networks, including scarce resources, erratic communications, unsupervised operations, and a lack of central management, these research projects still require improvement and adaptation to the WSN background [8].

Since data packets can be destroyed due to missing, interfernce, or sabotaged attacks, a valid SN is also required to conduct the DT operation [9, 10]. In order to safeguard the sent data packets from different types of attacks, security needs to be handled. Trust-based methods are helpful in today's WSN to combat malware nodes. In cyber security, trust is very crucial. In order to prevent the security threats of these hostile nodes, including invasions of privacy, data modification, and planning to organizing more complex attacks, it actively distinguishes between normal and hostile nodes and assesses the security status of SN based on their interactions and behaviours [11].

One of the most important drawback in complicated and unsecure WSN backgrounds is designing security procedures. Security in the DT process cannot be disregarded by researchers. The concepts of EC and security are contradictory. Designing security strategies in SN to safely transmit information to the base station (BS) is the task of strong security approaches. To preserve security in the DT process, SN is unable to operate robust and sophisticated security systems due to their limited energy resources.

To create an EE and lightweight trusted RP, security and EE must be combined when designing WSN protocols. In order to simultaneously accomplish security and EE, researchers have concentrated on CB trustworthy RP. To create a suitable and safe RP in WSN, researchers have also conducted extensive research. These techniques still require improvement

This work introduces a novel secure RP and tackles current research issues. By considering the restricted energy of nodes in WSNs, the strategy aims to improve network security. In order to accomplish this, a sophisticated RP that combines optimisation and deep learning (DL) approaches is suggested.

The Key Contributions are

- **The NSL-KDD dataset** is being used for WSN intrusion detection (ID).
- **PSO-FCM clustering** to optimize energy-efficient CH selection (CHS).
- **GNN-based classification** for identifying malicious nodes.
- **Symmetric butterfly optimization algorithm (SBOA) routing strategy** to enhance adaptive routing decisions.
- **Blockchain-based security** to safeguard network data transmission.

I. RELATED WORKS

Many studies in the field of AI-based ID systems (IDS) have focused on DL and ML techniques for anomaly detection in the past few years. An ML-based IDS that integrated LSTM and multivariate correlation analysis (MCA) was presented by the authors of [12]. The feature selection (FS) method named information-gain (IG) is utilized by this MCA-LSTM. The model then selects feature subset. With the NSL KDD dataset, 82.15% accuracy (ACC) was attained by MCA-LSTM in 5-way classification. The UNSW NB15's 10-way classification task has an ACC of 77.74% for the MCA-LSTM.

An effective multi-stage ML-based NIDS framework for NIDS assessment was later proposed by the authors in [13], using the RF and KNN procedures to classify different types of attacks. The Tree Parzen Estimator (TRE) is used to optimise the hyperparameters. The study's results showed that Bayesian optimisation (BO) with the TRE-optimized RF classifier had a higher detection ACC than other optimisation methods. Data sampling and FS are the two components of a hybrid data optimisation technique that is given. It is an optimal IDS based on this method, which they call DO_IDS. A technique that combines DL and flow computations for network attack detection was introduced by [14].

Using RNNs, an IDS based on DL was suggested in [15]. Their system's structure includes a data processing block. The categorical data was converted into numerical inputs by this block. Each input is then normalised using a scaling function, which restricts the ability of anomaly detection to identify specific attacks. In [16], a DL method for wireless ID uses a Feed-Forward Deep NN (FFDNN).

For enhancing security in WSN-IoT systems, ML with Firefly Algorithm (FA) was suggested by Karthikeyan et al. [17]. For enhancing security, novel optimization method was presented, and advancements in ID ACC by FA-ML are the 2

contributions offered by this analysis. By utilizing SVM model optimized with Grey Wolf Optimiser (GWO), FA-ML attains 99.34% ACC, 98.36% recall (R), and 96.67% f1-score. In the WSN-IoT systems, robust security mechanism is offered by the efficiency of the FA-ML method, and it was demonstrated by the outcomes.

To counter intelligent and frequent attacks in WSNs, especially Denial of Service (DoS) attacks, Salmi et al. [18] created an efficient IDS. The conventional IDS fails to detect complex attacks. Many DL-IDS methods are created that aims to detect DoS assaults in WSN. The four types of DoS attacks are Flooding, Scheduling, Blackhole, and Grayhole. These methods are trained using WSN-DS dataset. The CNN+RNN model's 85.19% P, 85.29% R, 82.34% f1-score, and 96.86% ACC demonstrated its noteworthy performance.

In order to improve WSN cybersecurity, a multi-criteria framework that use DL algorithms to assess risks according to context and severity was developed by Dontu et al [19]. In order to overcome issues including sluggish convergence, susceptibility to local optima, and a lack of population variety, the study presented the Enhanced Adaptive BOA (EABOA) for FS. In addition, a novel adaptive fragrance model that incorporates Lévy flight. Exploration is improved and local optima are avoided with Levy flight. An ACC of 94.76%, P of 86%, R of 80%, and an F-score of 80.06% were achieved by the model on WSN-DS, according to the experimental results.

II. PROPOSED METHODOLOGY

A novel RP for DT with longer WSN lifetime is introduced in this study. The data was preprocessed by Robust Scaling approach in order to train the DL module. Then a Cluster Head is selected using PSO-FCM Clustering. After then, the suggested Graph Neural Networks (GNNs) for classification with symmetric butterfly optimization algorithm (SBOA) for routing optimization route finding method had been effectively implemented. It effectively classifies the data via clustering. The procedure of the suggested method is shown in Fig. 1.

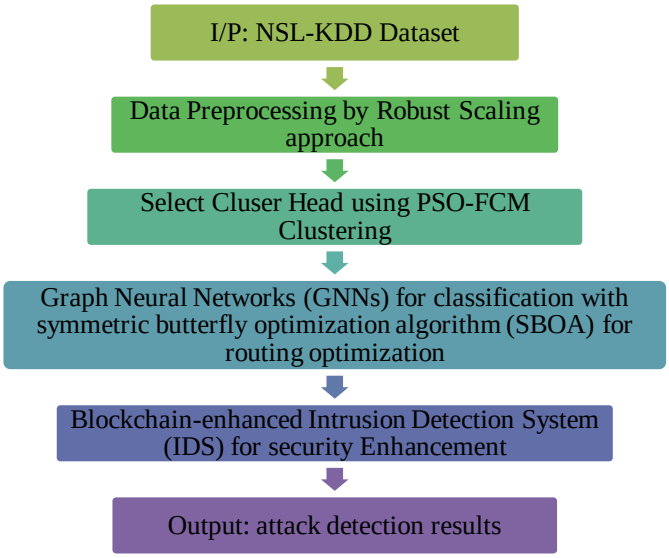

Figure 1: Proposed Block Diagram

A. Input Dataset

The data was gathered using the Data Gathering Block (DGB) from the NSL-KDD dataset, which is available at https://www.kaggle.com/datasets/hassan06/nslkdd. The NSL-KDD dataset contains attack-type labels in CSV format. In the original KDD dataset, there is an inverse link among the ratio of data selected from each difficulty grade class and the total count of data selected from each class. The detection rates of various ML procedures vary more, it is easier to accurately compare different learning methodologies. The experiments can be carried out on the whole set without the demand of arbitrarily choosing a subset because there are enough records in both the training and testing sets. Assessment outcomes from many research projects will therefore prove to be trustworthy and accurate.

B. Data preprocessing using Robust Scaling Method

An essential step of making the NSL-KDD dataset ready for ML applications, like ID in WSN, is data pre-processing. The robust scaling uses the median and the interquartile range (IQR) rather than the mean and standard deviation, it is especially helpful when the dataset contains outliers.

Robust Scaling transforms each feature **X** using the formula:

$$X_{Scaled} = \frac{X - median(X)}{IQR(X)} \quad (1)$$

Where:

- X_{Scaled}= Scaled feature value
- X = Original feature value
- $Median(X)$ = The middle value of the dataset (50th percentile)
- $IQR(X)$ = The IQR, calculated as:

$$IQR(X) = Q_3 - Q_1 \quad (2)$$

Where:

1st quartile (Q_1) equals 25th percentile. The 3rd quartile (Q_3), equals 75th percentile.

IQR represents the range where the central 50% of data lies. Since it ignores extreme values, it makes Robust Scaling effective for datasets with outliers.

C. Cluster Head Selection using Hybrid PSO-FCM

Clustering SN reduces EC and prevents overuse of certain nodes. Traditional clustering (LEACH, HEED) uses static clustering, which doesn't adapt to changing network conditions. In this work a Hybrid PSO-FCM balances energy efficiency and dynamic clustering. Here the efficient clustering process is reduces energy consumption by ensuring even load distribution among nodes. The main purpose of

- PSO (Particle Swarm Optimization) selects optimal Cluster Heads (CHs).
- FCM (Fuzzy C-Means) assigns sensor nodes to multiple clusters based on membership probability.

The PSO for CHS is here. In order to determine the ideal CH, the PSO considering the following aspects:

- Energy levels
- Node centrality
- Distance to base station

PSO is proposed based on the schooling and flocking patterns of fish and birds. When these two first started developing computer programming iterations of flocks circling food sources, they discovered how effectively their algorithms in handling optimisation problems.

PSO is computational methodology that enhances an issue in consistent, multidimensional search spaces (SS). PSO begins with swarm of irregular particles. All molecules are connected by velocity. The velocity of the particles is balanced with consideration of the past behaviour of each molecule and its neighbours when they pass through SS. Particles therefore have a tendency to migrate in the direction of better SS. The form of used PSO calculation is portrayed scientifically by accompanying conditions:

In each iteration, every particle modifies its own location and velocity using formulas (3) and (4).

$$v_{id}^{k+1} = \omega v_{id}^{k} + c_1\gamma_{1_1}\left(p_{id}^{k} - x_{id}^{k}\right) + c_2\gamma_{1_2}\left(p_{gd}^{k} - x_{id}^{k}\right) + \alpha(\text{rand} - \tfrac{1}{2}) \quad (3)$$

$$x_{id}^{k+1} = \begin{cases} 1 & s\left(v_{id}^{k+1}\right) > rand\ (0,1) \\ 0 & \text{else} \end{cases} \quad (4)$$

Here, S(vid) = 1/(1 + exp(−vid)),i = 1, 2, 3 ... m, sigmoid function id denoted as $s\left(v_{id}^{k+1}\right)$. The swarm particle count id denoted as m. The i^{th} particle's position at k^{th} iteration is denoted as x_{id}^{k}. The i^{th} particle's velocity at k^{th} iteration is represented as v_{id}^{k}. The i^{th} particle's optimal location is represented as p_{id}^{k}. Swarm's global best position is denoted as p_{gd}^{k}. Inertia weight is denoted as ω. Acceleration constants c1 and c2 usually lies between 0 and 2. Random value within the interval [0 1] are denoted as γ1 and γ2.

In feature space, every feature subset can be represented as a point. The subset with the highest classification accuracy and the shortest length is the optimal position. Each particle occupies a single position in the underlying swarm, which is randomly distributed throughout the SS. Particles are trying to get to the best location. In order to change their positions and find the local best position and global best position, they interact with one another during their breaks. Since they have the investigative capacity to execute FS and identify optimal subsets, they should finally merge on favourable, and possibly ideal locations.

The speed of every particle is shown as positive number; particle velocity is limited to a most extreme veocity Vmax. The number of features that should be altered to match the global best point is shown, velocity of particle advancing toward optimal location. The quantity of various features (bits) between two particles identified with contrast between their positions.

The particle location will be modernized by the novel velocity after the velocity has been updated. Let V be a novel velocity. In this case, the V bits of particles are modified arbitrarily and are not exactly the same as the Pg. Instead of essentially being the same as Pg, the particles at that moment fly towards global best and still discovering the SS. The global search (GS) capacity of particles is controlled by the Vmax imperative. While a smaller Vmax broadens local search (LS), a larger Vmax results in GS. Particles have trouble in leaving locally optimum locations when Vmax is low. Swarm may fly past best solutions if Vmax is set too high.

After performing PSO, FCM assigns each sensor a probability of belonging to multiple clusters. Because it allows flexibility when nodes move or energy levels change.

$$U_{ij} = \frac{1}{\Sigma_{k=1}^{c}\left(\frac{\|x_i - c_j\|}{x_i - c_k}\right)^{\frac{2}{m}-1}} \qquad (5)$$

Where:

- U_{ij} = Membership of node iii in cluster jjj
- C_j = Cluster center
- m = Fuzzification parameter

Hence the Outcome is that the PSO selects optimal CHs, and FCM assigns nodes dynamically, reducing energy consumption.

D. ID Using GNN

In this case, network data is modelled by GNNs as graphs. GNNs are perfect for ID in WSNs. GNNs are becoming more and more popular because of their special capacity to learn from graph-structured data by efficiently capturing network topology and node interactions through the transmission of messages between connected nodes. Different-level tasks, including node-level, edge-level, and graph-level prediction, can be handled by GNNs. The ID problem examined in this study is reduced to a binary classification task, which is part of the node-level prediction and involves determining whether a node v is being attacked (class 1) or not (class 0):

GNN uses the node features $\boldsymbol{x}_v$ and the graph structure (edges) E as inputs to learn a hidden representation, $\boldsymbol{h}_v$, for a node v in graph G. A message-passing and aggregation approach is used by the majority of sophisticated GNNs. In this case, the node's representation is modified by aggregating and learning data from itself and its neighbours after the data of one node is recursively transferred to the others along edges. One node could learn the data of other nodes in l hops when using a l-layered GNN to propagate messages. The latent representation at the GNN's l-th layer can be expressed as follows without sacrificing generality:

$$h_v^l = f^l(h_v^{l-1}, AGG^l(\{h_u^{l-1}, \forall u \in \mathcal{N}_v\})) \qquad (6)$$

The neighbouring nodes of node v are denoted by $\mathcal{N}_v$. Aggregations can range from simple ones like mean, max, and sum to more complicated ones like median, var, and std. They can even be exotic and learnable. The multi-layer perceptron (MLP) is an example of a function with learnable parameters, f^l. The kinds of graph operators are determined by the combination of $AGG^l$and f^l.
The output of the final hidden layer, such as a fully connected (FC) layer, could be sent directly to the output layer Φ for node-level prediction. It is sent to a readout function R with learnable parameters for graph-level prediction. The Φ can be formalised as follows:

$$h_v = \Phi(h_v^l) \qquad (7)$$

$$h_G = R(h_v^l | v \in V) \qquad (8)$$

Graph convolutional operator: Convolution for image classification is basically the same as graph convolution. A generalisation of convolution in Convolutional NN (CNN) is called graph convolution. Here, a hidden representation is learnt by combining the information of the central node (corresponding to the central pixel) with that of the neighbouring nodes (corresponding to nearby pixels). One way to formulate the graph convolution operation in [43] is as follows:

$$h_i' = \sigma(W^T \sum_{j \in \mathcal{N}_i \cup \{i\}} \frac{w_{ji}}{\sqrt{\hat{d}_j \hat{d}_i}} h_j) \qquad (9)$$

Here, the edge weight from source node *j* to target node *i* is indicated by $\hat{d}_i = 1 + \sum_{j \in \mathcal{N}_i} w_{ji}. w_{ji} \in \mathbb{R}$. The filter weight that needs to be optimised is **W**. σ denotes activation function. Transposition is denoted by *T*. Neighbouring nodes are equally important to the centre node because all edge weights are set to 1 by default. It is also possible to optimise edge weights to implicitly understand the significance of nearby nodes. As a result, it blocks compromised nodes and finds anomalies in routing decisions.

E. Dynamic Routing Optimization Using SBOA

In this research work a novel optimization technique of SBOA is introduced. Traditional routing algorithms (AODV, DSR) do not dynamically adjust to network conditions. SBOA optimizes routing and obtains the best path for transmission which helps to enhance the latency and energy efficiency. A search algorithm is used to illustrate the aforementioned discussions, and it is discovered that the butterfly (BF) display the following traits:

1. In order to attract one another, all BF are expected to release fragrances. 2. Each BF will either go at random or follow the best BF who is giving off the most fragrance. 3. The background of the objective function (OF) impacts or identify the stimulus intensity of a BF. The initialisation stage, the iteration stage, and the final stage are the three stages of BOA.

Every BOA run begins with the initialisation phase. In the final stage, searching is then carried out iteratively. When the best solution has been identified, the procedure is eventually stopped. The algorithm specifies the OF and its solution space throughout the initialisation stage. The parameters used in BOA are given values. Once the values are established, the procedure creates an initial population of BF for optimisation. A fixed size memory is allotted to store the data of the BF since their total number stays constant during the BOA simulation. The fragrance and fitness value (FV) of BF are computed and saved, and their placements in the SS are produced at random. This completes the initialisation stage, and the algorithm begins the iteration stage, which uses the generated artificial BF to do the search.

The algorithm goes through pre-defined set of iterations in the 2nd phase, often known as the iteration stage. Every iteration involves the relocation of every BF in solution space, followed by an evaluation of their FV. The fitness values of each BF at various locations in the solution space are first determined using the method. These BF will then generate fragrance in their respective areas using Eq. (10). The GS phase and the LS phase are the two main steps of the algorithm. Using Eq. (10), the BF moves nearer to the fittest butterfly/solution g∗ during the GS phase.

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i \qquad (10)$$

Here, the solution vector x_i for the i^{th} BF in t^{th} iteration is denoted by x_i^t. Out of all solutions in the current iteration, g∗ denotes the best one discovered thus far. f_i represents the i^{th} BF's fragrance.

In [0, 1], a random number that is denoted as r. The LS phase can be shown as

$$x_i^{t+1} = x_i^t + (r^2 \times x_j^t - x_k^t) \times f_i \qquad (11)$$

In the solution space, x_j^t and x_k^t represent the j^{th} and k^{th} BF. x_j^t and x_k^t are members of the same swarm. Eq. (11) then turns into a local random walk. Both local and global BF searches can be conducted for food and a mate. Food searching can account for a sizable amount of a BF's entire mating partner or food-tracking behavior, depending on physical proximity as well as other variables like wind, rain, etc. In order to transition from common GS to intensive LS, BOA uses a switch probability p.

The conventional BOA technique can effectively solve the problems. But, it faces few drawbacks like early convergence, easy slipping into local optima, and low performance. The S-BOA algorithm, which combines the BOA algorithm with the symmetric distraction factor (SDF), is used to overcome the issues with BOA.

- **Symmetric Distraction Factor (SDF)**

An innovative algorithm is provided to overcome these issues. This method uses a kind of association called SDF. SDF guides its neighbouring data towards its own. Both the spatial position of the neighbours, or distance attraction $\xi(0 < \xi < 1)$, that also depends on the nearby structure, and the data intensities, or feature attraction $\lambda(0 < \lambda < 1)$, form the basis of this SDF. The formulation of this SDF is as

$$sd^2(x_j, v_i) = \|x_j - v_i\|^2 (1 - \lambda H_{ij} - \xi F_{ij}) \quad (12)$$

Here, the feature attraction is represented by H_{ij}. The distance attraction is determined by F_{ij}. The two local attractions' levels are altered by the parameters λ and ξ. Hence SBOA finds optimal multi-hop routing paths, reducing latency and improving reliability.

F. Blockchain for Secure Communication

Once the optimal routing path is selected, blockchain is used to validate and secure the communication process. A blockchain ledger records the node authentication and routing decisions using cryptographic hashing. It enhances security by preventing unauthorized access, spoofing, and malicious intrusions. Each node in the WSN has a digital identity stored on a distributed blockchain ledger.

The transaction Verification is expressed as

$$H = SHA - 256(B_t + T_i + K_i) \quad (13)$$

where:

- H = cryptographic hash of the block.
- B_t = previous block hash.
- T_i = transaction data.
- K_i = authentication key.

This ensures tamper-proof security and authentication, preventing spoofing and unauthorized access.

III. RESULT AND DISCUSSION

The proposed Graph Neural Network (GNN)-based routing with Symmetric Butterfly Optimization Algorithm (SBOA) and Blockchain Security is validated through simulations using the NS2 simulator. The evaluation is performed by comparing the proposed approach against existing routing protocols, namely ASNGSRA, DMCNN, FRCSROD and CapsNets with EAMO techniques. To verify the efficacy of the suggested hybrid approach, performance evaluation metrics like ACC, P, R, F1-score, EE, and packet delivery ratio (PDR) are employed.

Security and Attack Resistance Analysis

Improving security and attack resistance in WSNs through the use of a GNN for data classification and Blockchain for authentication is one of the main goals of this research. Numerous network security risks, such as DoS, Remote-to-Local (R2L), and User-to-Root (U2R) assaults, are used to evaluate the approach. Security efficiency, false positive rate (FPR), and classification ACC are used to assess how well CapsNets with EAMO (Enhanced Adaptive Metaheuristic Optimisation) detect and mitigate cyberthreats.

$$\mathrm{P} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \times 100 \quad (14)$$

$$\mathrm{R} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \times 100 \quad (15)$$

$$\mathrm{F-measure} = 2 * \left(\frac{\mathrm{P} * \mathrm{R}}{\mathrm{P} + \mathrm{R}}\right) \quad (16)$$

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{FP} + \mathrm{TN} + \mathrm{FN}} \times 100 \quad (17)$$

The number of sensors, network area, data packet size, RP, transport protocol (TP), and mobility (M) are the simulation parameters that are presented in Table 1.

Table 1. Simulation parameter

Parameter	Value
Area	500*500
Nodes	100-1000
Energy	5J
Dimension	4096 bits
Routing Protocol	LEACH

TP	TCP
M	arbitrary

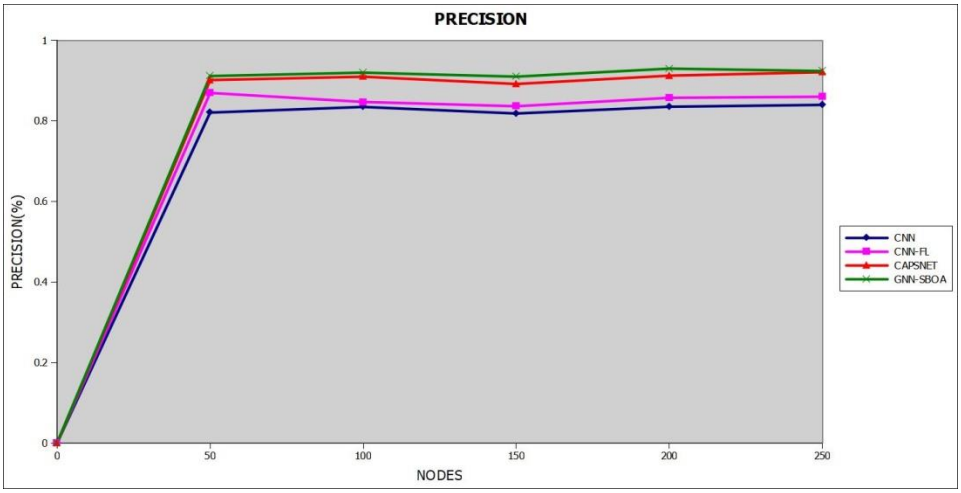

Fig. 2: Precision comparison

By contrasting the suggested GNN-SBOA technique with the CNN-FL, CapssNet, and basic CNN methods, the efficiency of suggested method is demonstrated. Fig. 2 demonstrates that GNN-SBOA outperforms CNN, CNN-FL, and CapsNet in precision analysis, proving its robustness in classification tasks. This validates the effectiveness of integrating graph-based learning with metaheuristic optimization for enhancing precision in cyber-physical system attack detection.

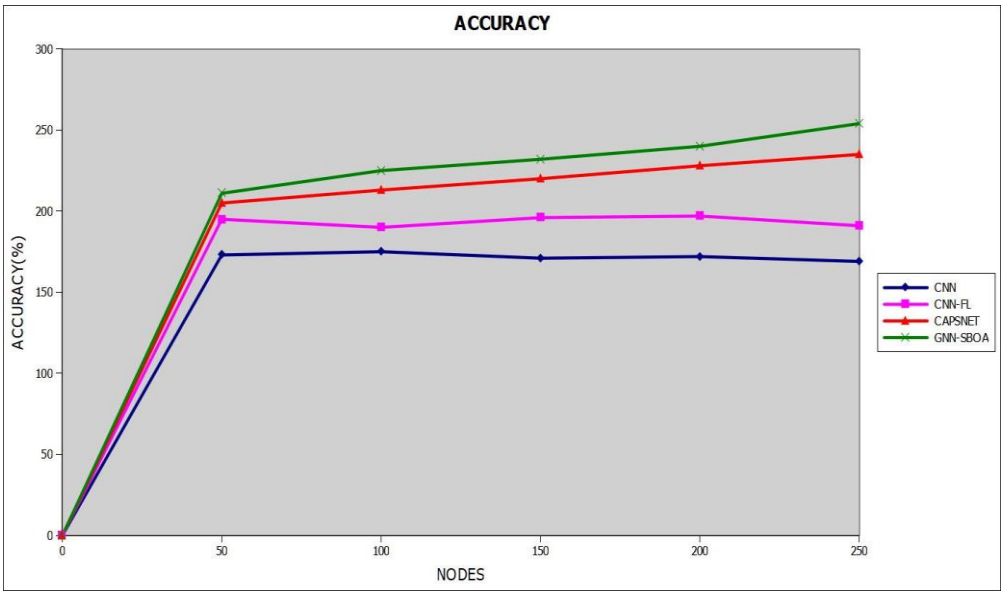

Fig. 3: Accuracy comparison

Fig. 3 demonstrates that GNN-SBOA significantly outperforms the other models in accuracy, validating its effectiveness in improving classification performance for cyber-physical system attack detection. The proposed GNN-SBOA model achieves 96% accuracy, outperforming all other models.

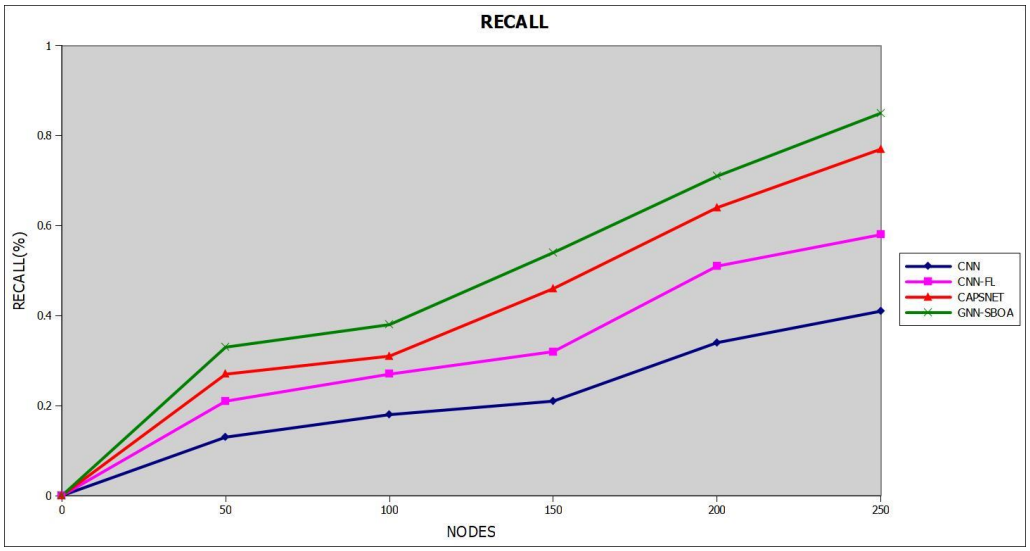

Figure 4: Recall score comparison

The suggested GNN-SBOA's performance is verified through comparison with the CNN-FL, CapsNets, and basic CNN techniques. Fig. 4 displays the R analysis experimental results.

When compared to other traditional methods like DT, RF, CNN, CNN-FL, and CapsNets, the suggested network offers improved security. In order to classify trust nodes and malware nodes, the suggested model can be used in real-time decision-making. The suggested GNN-SBOA model for the NSL-KDD dataset produced the improved detection ACC.

The simulation parameters specified in Table 1 are employed for assessing the SBOA efficiency. Using NGO methodologies, the performance of GNN-SBOA is verified by contrasting it with traditional RPs such ASNGSRA, DMCNN, FRCSROD, and CNN-Fl. To demonstrate the effectiveness of this suggested GNN-SBOA approach, the average PDR is assessed. Figure 5 then depicts the average PDR.

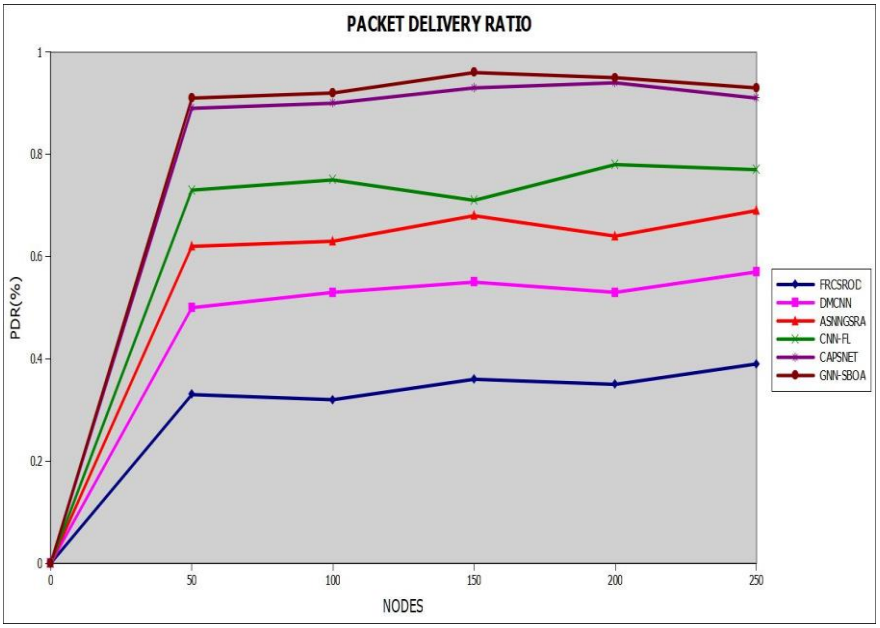

Fig. 5. Analysis of average PDR

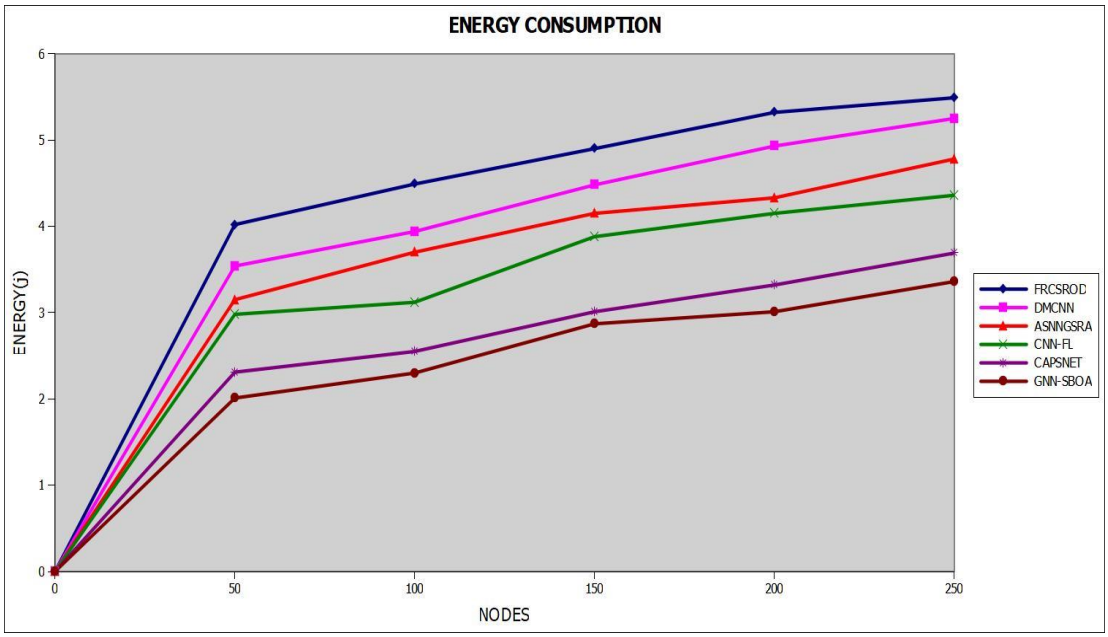

Fig. 6. Analysis of average EC

When compared to ASNGSRA, DMCNN, and FRCSROD approaches, the suggested GNN-SBOA model used less energy, as the above graph makes evident. It finds the best way to go to the sink node efficiently.

CONCLUSION

The proposed hybrid routing protocol successfully addresses the key challenges in WSN by integrating deep learning, optimization techniques, and blockchain-based security mechanisms. The incorporation of Robust Scaling for data preprocessing, PSO-FCM clustering for optimal Cluster Head (CH) selection, GNN for accurate data classification, and SBOA for dynamic routing optimization ensures a balanced approach to enhancing data transmission, energy efficiency, and network security. Additionally, the blockchain-based authentication mechanism fortifies the system against cyber threats, ensuring a secure and reliable communication framework. Simulation outcomes confirm that the suggested technique significantly extends the operational lifespan of WSNs compared to conventional approaches, demonstrating superior QoS, reduced energy consumption, and improved routing efficiency. In addition to providing a scalable and reliable foundation for next-generation WSN applications in many domains, including healthcare, smart infrastructure, and environmental monitoring, this comprehensive solution optimises numerous performance parameters simultaneously.

REFERENCES

1. Yousefpoor, M. S. & Barati, H. Dynamic key management algorithms in wireless sensor networks: A survey. Comput. Commun. 134, 52–69. https://doi.org/10.1016/j.comcom.2018.11.005 (2019).
2. Yousefpoor, M. S. & Barati, H. DSKMS: A dynamic smart key management system based on fuzzy logic in wireless sensor networks. Wirel. Netw. 26(4), 2515–2535. https://doi.org/10.1007/s11276-019-01980-1 (2020).
3. Rahmani, A. M. et al. An energy-aware and Q-learning-based area coverage for oil pipeline monitoring systems using sensors and Internet of Things. Sci. Rep. 12(1), 9638. https://doi.org/10.1038/s41598-022-12181-w (2022).
4. Temene, N., Sergiou, C., Georgiou, C. & Vassiliou, V. A survey on mobility in Wireless Sensor Networks. Ad Hoc Netw. 125, 102726. https://doi.org/10.1016/j.adhoc.2021.102726 (2022).
5. Esmaeili, H., Bidgoli, B. M. & Hakami, V. CMML: Combined metaheuristic-machine

learning for adaptable routing in clustered wireless sensor networks. Appl. Soft Comput. 118, 108477. https://doi.org/10.1016/j.asoc.2022.108477 (2022).
6. Rahmani, A. M. et al. An area coverage scheme based on fuzzy logic and shuffled frog-leaping algorithm (SFLA) in heterogeneous wireless sensor networks. Mathematics 9(18), 2251. https://doi.org/10.3390/math9182251 (2021).
7. Manuel, A. J., Deverajan, G. G., Patan, R. & Gandomi, A. H. Optimization of routing-based clustering approaches in wireless sensor network: Review and open research issues. Electronics 9(10), 1630. https://doi.org/10.3390/electronics9101630 (2020).
8. El Khediri, S. Wireless sensor networks: A survey, categorization, main issues, and future orientations for clustering protocols. Computing 104(8), 1775–1837. https://doi.org/10.1007/s00607-022-01071-8 (2022).
9. Jamshed, M. A., Ali, K., Abbasi, Q. H., Imran, M. A. & Ur-Rehman, M. Challenges, applications and future of wireless sensors in Internet of Things: A review. IEEE Sens. J.https://doi.org/10.1109/JSEN.2022.3148128 (2022).
10. Yu, X. et al. Trust-based secure directed diffusion routing protocol in WSN. J. Ambient Intell. Humaniz. Comput.https://doi.org/10.1007/s12652-020-02638-z (2022).
11. Selvaraj, A., Patan, R., Gandomi, A. H., Deverajan, G. G. & Pushparaj, M. Optimal virtual machine selection for anomaly detection using a swarm intelligence approach. Appl. Soft Comput. 84, 105686. https://doi.org/10.1016/j.asoc.2019.105686 (2019).
12. Dong RH, Li XY, Zhang QY, Yuan H (2020) Network intrusion detection model based on multivariate correlation analysis-long short-time memory network. IET Inf Secur 14(2):166–174
13. Injadat M, Moubayed A, Nassif AB, Shami A (2020) Multi-stage optimized machine learning framework for network intrusion detection. IEEE Trans Netw Serv Manag 18(2):1803–1816
14. Zhang H, Li Y, Lv Z, Sangaiah AK, Huang T (2020) A real-time and ubiquitous network attack detection based on deep belief network and support vector machine. IEEE/CAA J Autom Sin 7(3):790–799
15. Yin C, Zhu Y, Fei J, He X (2017) A deep learning approach for intrusion detection using recurrent neural networks. IEEE Access 5:21954–21961
16. Kasongo SM, Sun Y (2020) A deep learning method with wrapper based feature extraction for wireless intrusion detection system. Comput Secur 92:101752
17. Karthikeyan, M., Manimegalai, D. & RajaGopal, K. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. *Sci. Rep.* **14**(1), 231 (2024).
18. Salmi, S. & Oughdir, L. Performance evaluation of deep learning techniques for dos attacks detection in wireless sensor network. *J. Big Data* **10**(1), 17 (2023).
19. Dontu, S., Vallabhaneni, R., Addula, S. R., Pareek, P. K. & Hussein, R. R. Enhanced adaptive butterfly optimizer based feature selection for protecting the data in industry based WSN. In 2024 International Conference on Intelligent Algorithms for Computational Intelligence Systems (IACIS), 1–6 (2024). IEEE.
20. Sun, Z., Teixeira, A. M., & Toor, S. (2024, July). GNN-IDS: Graph Neural Network based Intrusion Detection System. In Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-12).