International Journal of Data Science and Artificial Intelligence (IJDSAI)
Volume 02, Issue 02, March – April (2024)

RESEARCH ARTICLE

HYBRID OPTIMIZATION INTEGRATED INTRUSION DETECTION SYSTEM IN WSN USING ELMAN NETWORK

B. Muthu Kumar [1, *], J. Ragaventhiran [2] and V. Neela [3]

[1] Professor, School of Computing and Information Technology, REVA University, Bangalore, India.
[2] Professor, School of Computing and Information Technology, REVA University, Bangalore, India.
[3] Assistant Professor, School of Computing and Information Technology, REVA University, Bangalore, India.

[*]Corresponding e-mail: muthu122@gmail.com

Abstract – Wireless Sensor Networks (WSNs) increases the usage of integrated systems and areas which attracts the attention of attackers. However, WSNs are vulnerable to different kinds of security threats and attacks. To ensure their security, an effective Intrusion Detection System (IDS) need to be in place to detect these attacks even under these constraints. The traditional IDS are less effective as these malicious attacks are becoming more intelligent, frequent, and complex. To overcome these challenges, this paper proposes a novel Improved Deep Neural Network Integrated Intrusion Detection System in WSN (IIDS-NET) technique has been proposed, which increases the energy efficiency in the WSN network. Initially, an optimal CH is selected via Tom and Jerry optimization algorithm (TJOA) based on the Residual energy and Node Centrality. The proposed scheme makes use of Improved Elman Spike Neural Network (IESNN) technique is implemented to detect the intrusion nodes and to blocks the suspicious or malicious activity in the wireless networks. Finally, the Aquila-Sooty Tern Optimization Algorithm (AQSOA) is used to find the optimal route for sending the data between the sensor nodes and the base stations. The proposed scheme is simulated by using Cloud simulator (CloudSim) and a comparison is made between proposed IIDS-NET and existing approaches such as GWOSVM-IDS, EPK-DNN, FL-SCNN-Bi-LSTM and SG-IDS in terms of detection accuracy, energy consumption, and throughput. The proposed HOPI-NET approach outperforms the existing techniques such as GWOSVM-IDS, EPK-DNN, FL-SCNN-Bi-LSTM and SG-IDS in terms of energy consumption of 120.73%, 198.68%, 193.34%, 187.73%, and 165.88% respectively.

Keywords *– Wireless Sensor Network, Internet of Things, Tom and Jerry Optimization, Improved Elman Spike Neural Network, Aquila-Sooty Tern Optimization.*

1. INTRODUCTION

Wireless sensor nodes (WSNs) locate themselves in the region of interest, where they monitor physical quantities close to their source and produce incredibly comprehensive data. Usually, the sensor nodes carry out one or two preprocessing measurements before sending the data to the cloud system or other central services for additional processing [1]. The data will eventually be passed to statistical machine learning or other techniques in these central services in order to obtain insights. Nevertheless, sample data may diverge from expected or previously taught "normal" behavior during analysis [2].

Due to the fact that sensor nodes can be put anywhere in the environment and are frequently needed to broadcast packets, a hostile attacker can easily get access to a wireless sensor network (WSN) [3,4]. Due to their open and distributed architecture, WSNs are crucial for many applications, but they also carry a high risk of cyberattacks. By seizing control of the sensor node, an attacker can send phishing messages, alter the veracity of data, listen in on conversations, and get access to network resources. The severity of these security flaws is made worse by the growing complexity and sophistication of morden malwares [5].

An intrusion detection system (IDS) is required to recognize known and unknown threats and promptly notify sensor nodes. An IDS is able to recognize unusual or suspicious activities and notify users when an intrusion takes place [6]. Furthermore, identifying attacker signatures in WSNs is unfeasible due to the absence of specialized datasets with parameters and common assaults. In order to mitigate their influence on WSN architecture, intrusion detection systems (IDS) for WSNs need to possess low computing overhead and exceptional precision in identifying intrusions [7].

The open, sparse architecture of WSNs and the constrained resources of sensor nodes make them susceptible to attacks. Nevertheless, WSNs require a substantial amount of work because they have limited resources, such as memory, processing power, and battery life. However, anomaly detection-based intrusion detection systems (IDS) utilize machine learning (ML) and often have a greater false positive rate (FPR) than earlier methods that rely on human signatures [8,9]. This means that it is challenging for ML anomaly-based systems to assess data and quickly spot infractions. Higher-dimensional training data is needed for these systems to overcome these restrictions, which increases the difficulty and duration of learning [10]. To address these shortcomings, a new and improved framework of Integrated Deep Neural Network Intrusion Detection System in WSN (IIDS-NET) has been proposed, which improves packet forwarding, lifetime network and node density while reducing the energy consumption and latency of sensor nodes. The main contributions of the proposed IIDS-NET framework are presented below.

- In the IIDS-NET framework, the optimization algorithm such as AQSTO, TJO and the IESNN DL approach is developed to recognize and avoid intrusion nodes, prolong network lifetime, and use less energy.
- Initially, an optimal CH is selected via Tom and Jerry optimization algorithm based on the Residual energy and Node Centrality.
- The proposed scheme makes use of IESNN technique is implemented to detect the intrusion nodes and to blocks the suspicious or malicious activity in the wireless networks.
- Finally, the Aquila-Sooty Tern Optimization algorithm is used to find the optimal route for sending the data between the sensor nodes and the base stations to establish a better communication.
- The accuracy, precision, recall, F-Score, throughput, and energy consumption are the parameters that are used to evaluate the efficiency of the proposed IIDS-NET strategy.

The rest of this article is divided into the following sections. Section 2 presents current related studies based on WSNs. Section 3 presents specifics of the proposed framework. Section 4 presents the result and discussions and Part 5 presents the conclusions and the future work.

2. LITERATURE SURVEY

Researchers have recently employed a variety of machine learning (ML) and deep learning (DL) approaches to assess intrusion detection systems and provide remedies to address the drawbacks and issues with conventional intrusion detection systems. Numerous methods have been developed in previous research to identify patterns in data and categorize instances into normal and abnormal groups. In this part, the literature on the most well-known IDS techniques will be discussed.

In 2021 Safaldin, M., et al [11] suggested a Deep neural network-based intrusion detection system for wireless sensor networks. The suggested GWOSVM-IDS method shortens the amount of time the environment allots for data processing while increasing speed and throughput. It accomplishes this by combining a support vector machine with a modified Wolf Gray binary optimizer. The NSL KDD99 dataset is used to assess the GWOSVM-IDS approach, which offers good detection accuracy in recognizing WSN intrusions.

In 2022 Gowdhaman, V. and Dhanapal, R., [12] suggested a Deep neural network-based intrusion detection system for wireless sensor networks. The suggested approach is predicated on a DNN structure that uses a cross-correlation procedure to choose the best characteristics for use in identifying intrusions. Tested on the NSL-KDD dataset, the suggested method achieves 95% detection accuracy and dramatically lowers the incidence of network intrusions.

In 2022 Otair, M., et al [13] suggested Enhanced swarm optimizer for wireless sensor networks, based on the intrusion detection system's gray wolf optimizer. The suggested approach selects features using a combination of Particle Swarm Optimization (PSO) and Gray Wolf Optimization (GWO) in order to detect intrusions. The suggested approach is assessed using the NSL KDD dataset, which optimizes the GWO algorithm as needed using K-means or SVM.

In 2023 Arkan, A. and Ahmadi, M., [14] suggested a decentralized, unsupervised, software-defined intrusion detection solution for wireless sensor networks. The SDWSN controller at various locations will get the data analysis results that are produced by clustering utilizing entropy and cumulative score similarity as criteria. The Cooja, WSN-DS, and NSL-KDD datasets are used to assess the effectiveness of the suggested technique, which yields a 97% detection rate for abnormal traffic.

In 2023 Raveendranadh, B. and Tamilselvan, S., [15] suggested an accurate technique for identifying threats in wireless sensor networks using kernel-centered exponential polynomial deep neural networks. Clustering and LS-BAT optimization are used by the EPK-DNN approach to locate features. In DL-K-Means, CH selection and other oriented hyrax optimization procedures are carried out. Using real-time BC and MC datasets, the suggested technique is tested, yielding results that meet the necessary detection accuracy of 97.21% and 96.86%, respectively.

In 2024 Bukhari, S.M.S., [16] suggested WSN for federated learning with SCNN-Bi-LSTM for safe intrusion detection to maintain privacy and boost dependability. The DL technique of the SCNN-Bi-LSTM model thoroughly investigates local and transient links in the model network in order to identify complicated and unknown cyber threats. Using the WSN-DS and CIC-IDS-2017 datasets, the FL-SCNN-Bi-LSTM approach exhibited a 99.9% classification accuracy.

In 2024 Saleh, H.M., [17] suggested a stochastic gradient descent-based machine learning intrusion detection system for wireless sensor networks. The SG-IDS technique uses the Gaussian Nave Bayes (GNB) and Stochastic gradient Descent (SGD) algorithms to search for intrusions in WSNs. The SG-IDS approach produces 98% precision, 96% recall, and 97% F1 measure with the WSN-DS dataset. Furthermore, it yielded accuracy scores of 0.87 and 1.00 for tasks linked to intrusion detection using the IoMT dataset.

The problem in WSN has limited resources. It is challenging to establish through an efficient IDS to prevent or mitigate these risks. Several approaches to effective CH selection were examined using the previously stated literature. The CHs threshold value is calculated without taking into account the ideal number of network clusters or other significant factors like residual energy and initiating energy. A novel IIDS-NET framework is proposed as a solution to combat these issues.

3. IMPROVED DEEP NEURAL NETWORK INTEGRATED INTRUSION DETECTION SYSTEM IN WSN

This paper proposes a novel Improved Deep Neural Network Integrated Intrusion Detection System in WSN (IIDS-NET) framework, which is developed to recognize and avoid intrusion nodes, prolong network lifetime, and use less energy. Initially, an optimal CH is selected via Tom and Jerry optimization algorithm based on the Residual energy and Node Centrality. The proposed scheme makes use of IESNN technique is implemented to detect the intrusion nodes and to blocks the suspicious or malicious activity in the wireless networks. Finally, the Aquila-Sooty Tern Optimization algorithm is used to find the optimal route for sending the data between the sensor nodes and the base stations to establish a better communication. The amount of energy usage, throughput, and detection accuracy are some of the parameters that are used to evaluate the effectiveness of the proposed strategy. The block diagram of the proposed method is given in Figure 1.

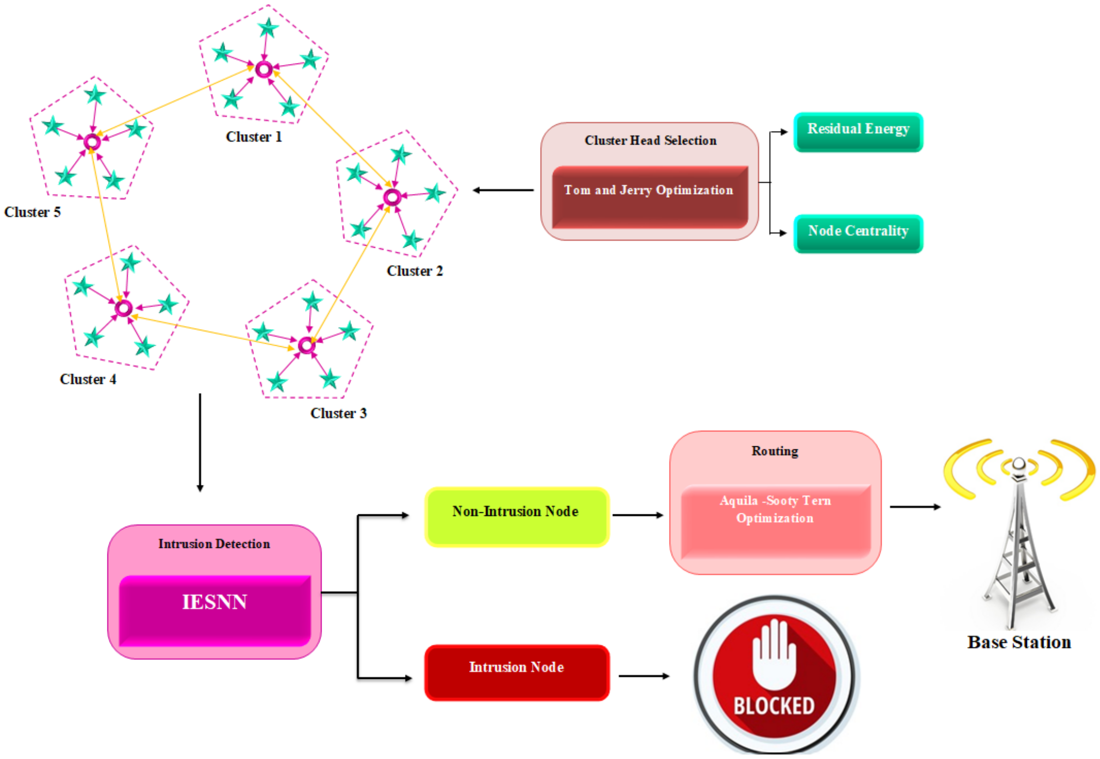

Figure 1. Block diagram of IIDS-NET Framework

3.1. CH selection Via Tom and Jerry Optimization Algorithm

This stage presents the optimization principles of Tom and Jerry (TJO) and then develops mathematical models for optimization issues. Based on comparable criteria like residual energy and node centrality, the CH is determined by utilizing the final source hops. The population can therefore be thought of as a collection of vectors whose values establish the problem's parameters. To ascertain the population of the rule set, equation (1) employs a single matrix known as the population matrix.

$$X = \begin{bmatrix} X_1 \\ \vdots \\ X_i \\ \vdots \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} X_{1,1} & \cdots & X_{1,d} & \cdots & X_{1,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i,1} & \cdots & X_{i,d} & \cdots & X_{i,m} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{N,1} & \cdots & X_{N,d} & \cdots & X_{N,m} \end{bmatrix}_{N\times m} \tag{1}$$

where dth is the issue variable that the search agent found. I, N represents the total population size, and m denotes the total number of problem variables. The values of the objective function are displayed in Equation 2.

$$F = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times m} \tag{2}$$

where Fi is the target item's cost for the ith search agent and F is the set of all potential values for the target. Equations (3) and (4), when solved, generate the ordered global matrix and the ordered objective function (5), respectively.

$$X^s = \begin{bmatrix} X_1^s \\ \vdots \\ X_i^s \\ \vdots \\ X_N^s \end{bmatrix}_{N\times m} = \begin{bmatrix} X_{1,1}^s & \cdots & X_{1,d}^s & \cdots & X_{1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i,1}^s & \cdots & X_{i,d}^s & \cdots & X_{1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{N,1}^s & \cdots & X_{N,d}^s & \cdots & X_{N,m}^s \end{bmatrix}_{N\times m} \tag{3}$$

$$F^s = \begin{bmatrix} F_1^s & \min(F) \\ \vdots & \vdots \\ F_N^s & \max(F) \end{bmatrix}_{N\times 1} \tag{4}$$

where Fs is the ordered vector of the objective function, Xs is the global matrix ordered by the objective function's value, and XiS is the ith member of the ordered global agent search matrix. Two populations such as mice and cats are suggested to be included in the TJO matrix. This is according to TJO. Equations (5) and (6) are the outcome of applying this idea to the computation of mouse and cat statistics.

$$M = \begin{bmatrix} M_1 = X_1^S \\ \vdots \\ M_i = X_i^S \\ \vdots \\ M_{Nm}=X^{S}_{\substack{1\\Nm}} \end{bmatrix}_{Nm\times m} = \begin{bmatrix} X_{1,1}^s & \cdots & X_{1,d}^s & \cdots & X_{1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{i,1}^s & \cdots & X_{i,d}^s & \cdots & X_{1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{Nm,1}^s & \cdots & X_{Nm,d}^s & \cdots & X_{Nm,m}^s \end{bmatrix}_{Nm\times m} \tag{5}$$

$$C = \begin{bmatrix} C_1 = X_{Nm+1}^S \\ \vdots \\ C_i = X_{Nm+j}^S \\ \vdots \\ C_{Nc}=X^{S}_{\substack{1\\Nm+Nc}} \end{bmatrix}_{Nc\times m} = \begin{bmatrix} X_{Nm+1,1}^s & \cdots & X_{Nm+1,d}^s & \cdots & X_{Nm+1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{Nm+j,1}^s & \cdots & X_{Nm+i,d}^s & \cdots & X_{Nm+1,m}^s \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ X_{Nm+Nc,1}^s & \cdots & X_{Nm+Nm,d}^s & \cdots & X_{Nm+Nm,m}^s \end{bmatrix}_{Nc\times m} \tag{6}$$

The cat population matrix is represented by M, the mouse population matrix by C, the cat population matrix by Nc, and the jth mouse is represented by M I respectively. As of right now, equations (7) through (8), reflect the TJO improvement strategy.

$$C_j^{new}: C_{j,d}^{new} = C_{j,d} + r \times \left(m_{k,d} - I \times C_{j,d}\right) \,\&\, j = 1:Nc, d = 1:m, k \in 1:Nm \tag{7}$$

$$I = round(1 + rand) \tag{8}$$

$$C_j = \begin{cases} C_j^{new} & | \, F_j^{c,new} \\ C_j, & , \quad |else \end{cases} < F_j^c \tag{9}$$

The updated status of the jth conversation is represented by Cj new, the updated value of the second issue variable received by the jth cat is represented by CJ, D new, and the updated value of the variable is represented by mk, D. The updated value of the target element function is represented by the value of the mouse's kth dimension and Fj c, new. Equations (10) through (11) demonstrate how Jerry's position is updated iteratively.

$$H_i: h_{i,d} = X_{I,d} \& i = 1: N_m, d = 1:m, I \in 1:N \tag{10}$$

$$M_i^{new}: m_{i,d}^{new} = m_{i,d} + r \times \left(h_{i,d} - I \times m_{i,d}\right) \times sign(F_i^m - F_i^H) \,\&\, i = 1: N_m, d = 1:m \tag{11}$$

$$M_i = \begin{cases} M_i^{new}, | \, F_i^{m,new} < F_i^m \\ \qquad M_i, |else \end{cases} \tag{12}$$

The ith mouse's targeting characteristic is represented by the symbol Fi H, and its hideaway location is represented by the sign H I. The ith Tom's recently acquired region is described as mi which describes the targeting feature's cost. The algorithm continues to the next iteration after each one ends when the stopping condition based on equations (9) to (12) is satisfied. Following the completion of all intervals in the optimization process, TJO will produce the optimal CH that is as near too ideal as possible.

3.2. Intrusion Detection via Improved Elman Spike Neural Network

The Improved Elman Spike Neural Network (IESNN) is used to identify intrusive nodes once the CHs have been chosen. In an Elman neural network, the topology consists of the hidden layer, input layer, context layer, and output layer. The context layer incorporates automatic feedback with configurable gain together with a dynamic feedback method that stores the hidden layer's prior outputs. Compute-intensive applications in embedded systems and edge devices are an ideal for IESN because of its low weight. Equation (15) displays the input layer and nodes as they are,

$$y_i^{(1)}(m) = f_i^{(1)}\left(net_i^{(1)}(m)\right); i = 1 \tag{13}$$

Let $net_i^{(1)}(m) = e_i^{(1)}(m) : n$ represents the n th iteration, $e_i^{(1)}(m)$ as input, $y_i^{(1)}(m)$ as an outcome of the initial layer. The IESNN dynamics is labeled in equation (14)-(16),

$$NS(y) = NLF\left(W_{con*inv} NS_{con(y),} W_{in*inv} input(y)\right) \tag{14}$$

$$NS_{con(y)} = \alpha(y) NS_{con}(y-1) + W * NS(y-1) \tag{15}$$

$$Output(y+1) = W_{inv*out} NS(y) \tag{16}$$

where the nonlinear function NLF(.) specifies how to categorize and display IESNN. By output (y), the associated input and output are implied. The state node vector represents NS(y) and NSCon(y) for context layers and hidden layers, respectively. More response self-connection is indicated by the phrases “win∗inv” and “wcon∗inv” which denote neurons connected to weights from the data layers to the buried layers. A formula that represents a node in the hidden layer.

$$y_j^{(2)}(n) = S\left(net_j^{(2)}(n)\right); j = 1, \dots 9 \tag{17}$$

$$net_j^{(2)}(n) = \textstyle\sum_i W_{in*inv} \times y_i^{(1)}(n) + \sum_k W_{con*inv} \times y_k^{(3)}(n); k = 1 \dots .9 \tag{18}$$

Where $S\left(net_j^{(2)}(n)\right)$ indicated, the function in the sigmoid, $y_i^{(1)}$, $y_k^{(3)}(n)$ represents the data from the input and hidden layer and $y_j^2(n)$ represents the outcome of the layer that is hidden. Next, nodes in the context of the level are denoted by equations for the layer.

$$y_k^{(3)}(n) = \alpha y_k^{(3)}(n-1) + y_j^{(2)}(n-1) \tag{19}$$

To accurately detect intrusive nodes, interpret this as a rise in the update self-connection response in the context layer. In a single layer IESNN, the hidden layer is composed of two input neurons, and only two neurons provide output. At the bottom of the output layer is a representation of the layer nodes' outcomes.

$$y_l^{(4)}(n) = f_l^{(4)}\left(net_l^{(4)}(n)\right) \tag{20}$$

$f_l^{(4)}$ indicate the parameter that is controlled by the presented IESNN approach,

$$net_l^{(4)} = \sum_j W_{inv*out} \times y_j^{(2)}(n) \quad (21)$$

where winv∗out stands for the neural weights connecting the neurons in the hidden layer. Statistics about connections are updated by the network. To make the last detection step better, apply the following equation.

$$W_{inv*out}^{y}(Time + 1) = W_{inv*out}^{y}(Time) - \eta . \delta_f . NS^{y} \quad (22)$$

The unit of time is "Time," and the learning rate is represented by η. wherein the neurons' threshold values verify that the IDS is classified according on the spike levels of each neuron within a specific time interval, or "Time." This demonstrates that, in comparison to normal, the threshold value of the neurons under consideration may detect the invasive node with effectiveness. If membrane potential g is greater than a given threshold value, it is categorized into distinct penetration groups. The delta function of a neuron, or δf, can be computed using the equation that follows.

$$\delta_f = \frac{Error}{\sum_{i=1}^{Niv} \sum_{y=1}^{NoD} W_{inv*out}^{y} \frac{\partial input}{\partial Time}} \quad (23)$$

The subsequent formula (24), which calculates the difference between the final neurons are,

$$Error = t_f^{DST} - Time_f^{NLF} \quad (24)$$

Where, t_f^{DST} indicates the duration of a neuron's spike $Time_f^{NLF}$ stands for the result of a neuron's actual spike timing.

3.3. Routing Via Aquila-Sooty Tern Optimization

The proposed design states that Aquila-Sooty Tern optimization is used for routing. The AQSTO algorithm's primary benefits are its simplicity of use, excellent detection capability, social behavior, and rapid convergence for the best BS selection. AQSTO uses comparable techniques to find unmonitored BSs. Using Aquila optimization, the fitness function for the optimal solution is first determined. The natural activity and method of existence of seabirds serves as the inspiration for the AQSTO algorithm, which is utilized as the routing method to detect BSs. In order to prevent impractical solutions, the user identification Q_j is assigned the starting position value of the ith index. If there is a 50% or greater resemblance between Q_i and Q_j. Nodes inside a cluster are distinct from one another but comparatively similar to nodes in other clusters.

Aquila optimization

Initially, Aquila optimization was used to calculate the fitness function for the optimal solution. Using equation (25), an initial m containing p solutions is produced.

$$A_{ij} = x_1 * (mq_j - nq_j) + mn_j , i = 1,2,3 \ldots x, j = 1,2, \ldots \ldots, Dim \quad (25)$$

In equation (28), the search space bounds are denoted by mqi and nqj. The random number x1 ∈ [0, 1] is represented, and the agent's dimension is Dim. Using equation (26), the fitness value of each cluster is determined.

$$f_V = \lambda + \delta + (1 - \lambda)\, X \left(\frac{|bA_i|}{x_{Dim}}\right) \quad (26)$$

Here in $|bA_i|$ values range from up to 0.5 for optimum solution.

Migrating Behavior

At this point, the best solution found using aquila optimization will be further optimized using AQSTO to determine the best course of action. Three guidelines are adhered to by Sooty Terns for a successful migration:

Collision avoidance: In order to prevent conflicts with other Search Agents in the nearby regions, the Search Agent's (SA) position is strategically planned.

$$a_{ij} = N_{ik} \times m_{ij}(p) \quad (27)$$

where p is the actual iteration, m_ij is the SA's current position, and a_ij is the SA's position to avoid collisions with other SAs. N_ik is the SA's position at a given time in the search space specific to the search space.

Converge in the direction of best neighbor: In order to prevent collapses the researchers advance toward the closest neighbor.

$$b_{ij} = X * (Y_{best}(P) - m_{ij}(p)) \quad (28)$$

X denotes the largest discovery, b_ij represents the search agent's various places, and m_ij represents the most appropriate search agent depending on the relevant criteria:

$$X = 0.5 \times R_{and} \quad (29)$$

where, R_and is a random number between [0, 1].

Update corresponding to best search agent: The STO framework has been enhanced with new methods based on quantum mechanical theory and orbital analysis. Quantum algorithms are utilized to update data via the following equations:

$$C_{ij}^{u+1} = S_{ij}^{u} \pm \alpha |Kbest_j^u - Z_{ij}^u| ln \frac{1}{x} \quad (30)$$

$$c_{ij}^{u+1} = \begin{cases} S_{ij}^{u} \pm \alpha |Kbest_j^u - Z_{ij}^u| ln \frac{1}{x}, & \text{if m and } (0,1) \geq 0.5 \\ S_{ij}^{u} \pm \alpha |Kbest_j^u - Z_{ij}^u| ln \frac{1}{x}, & \text{otherwise} \end{cases} \quad (31)$$

By adjusting their positions, search agents can eventually get higher.

$$c_{ij} = \rho c_{ij} + (1 - \rho) c_{tj} \quad (32)$$

where C_ij denotes the region with the highest fitness value between the hunter agent and the search agent.

Attacking Behavior

Using similarity criteria, the optimal path is chosen in this step. These birds can go farther on their migration. Using analysis, the following behavior can be inferred:

$$l = S_{radius} \times sin(i) \quad (33)$$

$$m = S_{radius} \times cos(i) \quad (34)$$

$$n = S_{radius} \times j \tag{35}$$

$$D = a \times e^{kb} \tag{36}$$

where e is the base of the natural logarithm, i denotes that the variable is in the range 0-1, b and an are constant variables that represent the spiral, and radius S is the radius of each spiral. With constant values of 1 for a and b, SA is thus in the updated position.

$$V_{ij}(p) = (C_{ij} \times (l + m + n)) \times Y_{best}(P) \tag{37}$$

Consequently, V_ij(p) returns the optimal solution with BS after updating the positions of other SAs. After multiplying the input by the feature vector, a random subset of nodes is added. In order to determine the next route, the fully connected layer (FC) can receive the final STO algorithm, which is constructed based on the detected BS during movement and attack operations. Based on the output of the preceding layer, the FC layer groups linked nodes using different cluster STO methods.

4. RESULT AND DISCUSSION

A cloud simulator is used in the proposed method's implementation to assess its efficacy. The proposed framework's effectiveness is assessed using the techniques that are currently in use. Various nodes employ performance indicators such as throughput, power consumption, and detection accuracy. Table 1 displays the inputs used in the simulation.

Table 1. Simulation Parameters

Simulation Parameters	Values
Base Station Position	200, 200
Energy Consumed by Circuit	50 nJ/bit
Energy Consumed in Empty Space	10 pJ/bit/m^2
Energy Consumed for Data Aggregation	5 nJ/bit
Energy Consumed by Multipath Channel	0.0013 pJ/bit/m^4
Initial Energy	20 J
Number of Sensor Nodes	500
Simulation Area	400 X 400 m^2
Simulation Time	120 sec
Speed of Mobile Sink	25 m/s
Threshold Energy	0.1 mJ

4.1. Dataset Description

The ToN-IoT dataset is a comprehensive dataset that was just provided by the Advanced Computing and Communications Society (ACCS) in 2019. It makes use of a portion of network data gathered throughout the ecosystem. Attack instances with a rate of 796,380 benign flows to 21,542,641 attack threads, for a total of 22,339,021 threads, are mostly included in the IoT status. The Bro-IDS utility was used to remove 44 of its original functionalities.

4.2. Performance Measures

Five fundamental evaluation criteria, including precision, detection rate, recall, and F-Score, are used in this research. The precision rate is a tool for assessing how precise a mold is in making future predictions.

$$Accuracy = \frac{TN+TP}{N_n+N_P} \tag{38}$$

$$Precision = \frac{TP}{FP+TP} \tag{39}$$

$$Recall = \frac{TP}{N_P} \tag{40}$$

$$F - Score = \left[2 * \left\{\frac{Precision*Recall}{Precision+Recall}\right\}\right] * 100 \tag{41}$$

$$T_p = \frac{Received\ packet\ size}{stop\ time - start\ time} \tag{42}$$

$$E_c = \sum_{i=1}^{N} E_{i,L} \tag{43}$$

The variables in this equation are: FN, FP, and TP, which stand for the number of instances that were initially normal but were deemed aggressive cases, potentially attacked instances, and initially normal instances and TN indicates the number of initial typical instances that are anticipated to be typical cases.

4.3. Comparative Analysis

Figure 2 displays the energy consumption analysis of the proposed IIDS-NET method utilizing several techniques. Between 100 to 500 connections are present. In comparison to other existing routing techniques, the IIDS-NET method that has been proposed offers superior energy consumption performance. The proposed IIDS-NET framework's 200 nodes use 120.73% less electricity. Additional techniques that produce power consumption values include SG-IDS-, FL-SCNN-Bi-LSTM-187.73%, EPK-DNN-193.34%, and GWOSVM-IDS-198.68% and SG-IDS-165.89% respectively increasing the number of nodes also results in increased power consumption.

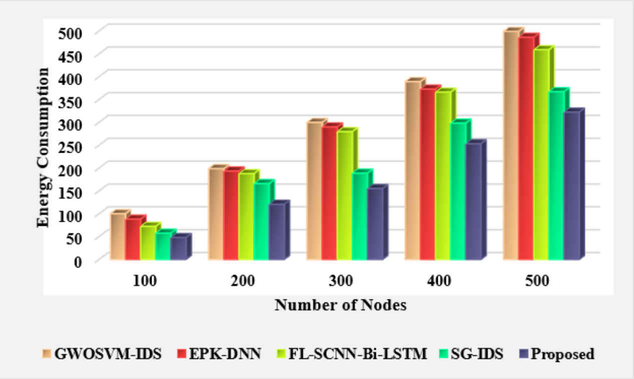

Figure 2. Energy consumption Analysis

Figure 3 compares the proposed IIDS-NET throughput analysis to alternative methods. In terms of throughput, the proposed IIDS-NET approach outperforms the alternatives. All approaches have a decreasing throughput value as the total number of nodes increases. Using the proposed approach, initial throughput for node 100 is 97%. The investigation indicates that the proposed IIDS-NET approach transmits data more rapidly. With SG-IDS, throughput performance decreases.

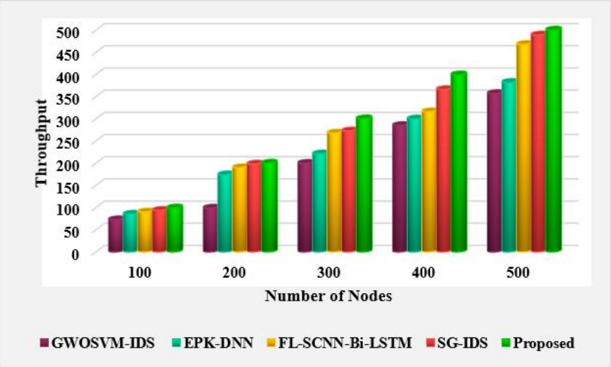

Figure 3. Throughput Analysis

5. CONCLUSION

This paper proposes a novel Improved Deep Neural Network Integrated Intrusion Detection System in WSN (IIDS-NET) framework, which is developed to recognize and avoid intrusion nodes, prolong network lifetime, and use less energy. The proposed framework is validated by using cloud simulator. A comparison is made between proposed IIDS-NET and existing approaches such as GWOSVM-IDS, EPK-DNN, FL-SCNN-Bi-LSTM and SG-IDS in terms of detection accuracy, energy consumption, and throughput. The proposed HOPI-NET approach outperforms the existing techniques such as GWOSVM-IDS, EPK-DNN, FL-SCNN-Bi-LSTM and SG-IDS in terms of energy consumption of 120.73%, 198.68%, 193.34%, 187.73%, and 165.88% respectively. Future research will concentrate on cutting-edge AI methods to address urgent problems with connection compatibility and link security. In order to maintain adequate defenses against routing assaults, new solutions will also be put out to solve attack mitigation difficulties via current intrusion detection systems.

CONFLICTS OF INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

FUNDING STATEMENT

Not applicable.

ACKNOWLEDGEMENTS

The author would like to express his heartfelt gratitude to the supervisor for his guidance and unwavering support during this research for his guidance and support.

REFERENCES

[1] S. Muthukumar, A. Hevin Rajesh, and D. Jenice Prabhu, "Reduancy aware dynamic routing protocol using salp swarm optimization algorithm", *International Journal of System Design and Computing*, vol. 01, no. 01, pp. 35-42, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] S. Siva Shankar, B.T. Hung, P. Chakrabarti, T. Chakrabarti, and G. Parasa, "A novel optimization based deep learning with artificial intelligence approach to detect intrusion attack in network system", *Education and Information Technologies*, pp. 1-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] K. B. Shah, S. Visalakshi, and R. Panigrahi, "Seven class solid waste management-hybrid features based deep neural network," *International Journal of System Design and Computing*, vol. 01, no.01, pp. 1-10, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] R.B. Kagade, and S. Jayagopalan, "Optimization assisted deep learning-based intrusion detection system in wireless sensor network with two-tier trust evaluation", *International Journal of Network Management*, vol. 32, no. 4, pp. e2196, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] A. Agasthian, Rajendra Pamula, and L.A. Kumaraswamidhas, "Integration of monitoring and security based deep learning network for wind turbine system," *International Journal of System Design and Computing*, vol. 01, no. 01, pp. 11-17, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] S. Godala, and M.S. Kumar, "A weight optimized deep learning model for cluster-based intrusion detection system", *Optical and Quantum Electronics*, vol. 55, no. 14, pp. 1224, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] R. Sheeja, and R. Nishant, "Reduction in greenhouse gas emission by using sustainable transportation systems to increase the environmental and economic benefits", *International Journal of System Design and Computing*, vol. 01, no.01, pp. 18-25, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] G. Vembu, and D. Ramasamy, "Optimized deep learning-based intrusion detection for wireless sensor networks", *International Journal of Communication Systems*, vol. 36, no. 13, pp. e5254, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] M. B. Asha Stebi, and A. Jeyam, "Estimation of household appliances and monitorization for impact reduction using electro chemical sensor", *International Journal of System Design and Computing*, vol. 01, no.01, pp. 26-34, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] S. Karthic, and S.M. Kumar, "Hybrid optimized deep neural network with enhanced conditional random field-based intrusion detection on wireless sensor network", *Neural Processing Letters*, vol. 55, no. 1, pp. 459-479, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks", *Journal of ambient intelligence and humanized computing*, vol. 12, pp. 1559-1576, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] V. Gowdhaman, and R. Dhanapal, "An intrusion detection system for wireless sensor networks using deep neural network", *Soft Computing*, vol. 26, no. 23, pp. 13059-13067, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[13] M. Otair, O.T. Ibrahim, L. Abualigah, M. Altalhi, and P. Sumari, "An enhanced grey wolf optimizer-based particle swarm optimizer for intrusion detection system in wireless sensor networks", *Wireless Networks*, vol. 28, no. 2, pp. 721-744, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[14] A. Arkan, and M. Ahmadi, "An unsupervised and hierarchical intrusion detection system for software-defined wireless sensor networks", *The Journal of Supercomputing*, pp. 1-27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] B. Raveendranadh, and S. Tamilselvan, "An accurate attack detection framework based on exponential polynomial kernel-centered deep neural networks in the wireless sensor network", *Transactions on emerging telecommunications technologies*, vol. 34, no. 3, pp. e4726, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] S.M.S. Bukhari, M.H. Zafar, M. Abou Houran, S.K.R. Moosavi, M. Mansoor, M. Muaaz, and F. Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for

enhanced reliability", *Ad Hoc Networks*, vol. 155, pp. 103407, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] H.M. Saleh, H. Marouane, and A. Fakhfakh, "Stochastic Gradient Descent Intrusions Detection for Wireless Sensor Network Attack Detection System Using Machine Learning", *IEEE Access*, 2024. [CrossRef] [Google Scholar] [Publisher Link]

AUTHORS

B. Muthu Kumar Professor, School of Computing and Information Technology, REVA University, Bengaluru received his B. E (CSE) degree from Anna University, Chennai in the year 2005, M. Tech (CSE) (Gold Medalist) received from Dr. MGR. University, Chennai in the year 2007 and Doctoral degree from St. Peter's University, Chennai in the year 2013. He is having more than 16 years of teaching experience in reputed engineering colleges. He has published more than 40 peer reviewed International Journals, 50 International/National Conference and attended more than 150 Workshops/FDPs/Seminars etc., He organized many events like Conference/FDPs/Workshops/Seminars/Guest Lecture. He has published more than 10 patents in various fields like Wireless Sensor Networking, Image Processing, Optimization Techniques and IoT. He received nearly 5.67 Lakhs funding from various agencies like AICTE, ATAL and IEI. He has written 2 books from reputed publishers. He received Best Researcher Award in the year 2021 and Innovative Research and Dedicated Professor Award in Computer Science and Engineering in the year 2018. He has professional membership on ISTE, CSI, IEI, IACSIT, IAENG, CSTA, and SIAM. He has invited as Guest Lecture / Chairperson / Examiner / Reviewer/Editorial Board Member in various Institutions/Journals/Conferences. He is a recognized supervisor in Anna University, Chennai and currently guiding 4 research scholars. His areas of interest are Image Processing, Wireless Networks, IOT and Computing Techniques.

J. Ragaventhiran received his Ph. D from Anna University, Chennai, India, M.E degree in Computer Science and Engineering from Anna University, Chennai from Madurai Kamaraj University and Anna University, Tamil Nadu, India in 2002 and 2008 respectively. He is currently pursuing PhD in the Department of Information and Communication Engineering in Anna University, Chennai, Tamil Nadu, India and B.E Computer Science and Engineering from Madurai Kamaraj University, Tamil Nadu, India. He is currently working as a Professor in School of Computing and Information Technology, REVA University, Bengaluru, India. His research interest includes Data Mining, Big Data, Machine Learning. He is a life member in Computer Society of India (CSI) and Institution of Engineers (IEI) India. He has reviewed and chaired various national and international conferences including IEEE conferences.

V. Neela Working as Assistant professor, School of Computing and Information Technology, Reva University, Kattigenahalli, Bangalore-560064.She completed her B. Tech in Information Technology in AMIETE and her M. Tech in Reva University, she is having 6yrs of experience in corporate sector as Business Analyst and 2 Yrs. of experience as Assistant Professor currently working in REVA University Her research interest includes Image Processing, cloud computing, Data Mining and Big data.

Arrived: 14.03.2024

Accepted: 22.04.2024