International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 27, No. 5, October, 2022, pp. 685-693
Journal homepage: http://iieta.org/journals/isi

An Optimal Cluster Head Selection with Trusted Path Routing and Classification of Intrusion in WSN Employing CHLNNet

Mustafa Amer Obaid[1], Alaa Sabree Awad[2*], Ibrahim Saud Khaleel[3]

[1] College of Medicine, University of Anbar, Ramadi 31001, Iraq
[2] College of Basic Education, University of Anbar, Ramadi 31001, Iraq
[3] Anbar Vocational Education Department, General Directorate of Education Anbar, Ramadi 31001, Iraq

Corresponding Author Email: abosaadpro@uoanbar.edu.iq

https://doi.org/10.18280/isi.270501

Received: 14 July 2022
Accepted: 6 October 2022

Keywords:
intrusion detection, neural network, classification, cluster head, trust management, optimal route

ABSTRACT

A wireless sensor network consists of a large number of sensors dispersed across a large area. These are used in broad areas including queue management, military applications, ecological applications, and others. This method, which combines deep learning and optimisation strategies with a focus on attack identification, is still under testing. The nodes will first be distributed randomly, centred on the network's dimension, under a system paradigm. Comparison sets are produced by use of an energy-related timer. Later, the geographical comparison, the quality of the link between the cluster head (CH) and cluster member (CM) nodes, and the node's remaining network energy will all be taken into account when analysing the transmission probability. The CH will determine how to manage the trust. The node will be chosen as CH after it meets the criteria for trust coverage. This will be chosen as CM if the situation is still unsatisfactory. The Dempster-Shaft theory and multi-dimensional trust criteria will be used to determine the cluster pathways' (CP) optimal range for effective data transfer, with residual energy and distance being the key constraints. Cascaded Hermite Laguerre Neural Network will classify and identify the attack if the best and most reliable path is still chosen (CHLNNet). This proposed approach will be compared against three sophisticated methodologies with regard to several parameters. As a result, the suggested CHLNNet technique achieves 91.4% of malicious detection rate, 28.2% average latency, 94.8% throughput, 23% end-to-end delay, and 31.4% routing overhead.

1. INTRODUCTION

Since the past decennary, the analysts collected extra knowledge in the security discipline in wireless sensor networks (WSNs) [1]. WSN remains a sensor nodes' (SNs) set linked to one another and are sensed in specific settings [2]. This contains the advantages of restricted power utilization, little dimension, and inexpensiveness. This remains employed in disparate disciplines like satellite communication, battleground surveillance, medical aid, ocean excerpting, and so on [3]. WSNs' framework will be fundamentally split into Flat and Clustered frameworks [4].

There remain several attacks initiated by the attackers at the initial 3 layers – physical, MAC, and network layers. Concerning the first one, the attackers jam the manual path by radio frequency dispensation thereby causing the transfer issue. In the second one, the attackers generate a collision and immoral channel precedence for the connection institution [5]. Lastly, the third one disorders the routing and data flow (DF) management; these attacks happen in the network including black hole attack, wormhole attack, sinkhole attack, selective forward attack, and Sybil attack. Hence, security problems remain unresolved problems within the WSNs [6]. Lately, many security systems are modeled to identify the malevolent actions in the network named intrusion detection system (IDS). It could identify the intruder within the WSNs. It indicates the SNs' atypical actions to the rest of the nodes within the network. There remain 2 IDS kinds employed – anomaly detection system (DS) and misuse DS [7].

WSN's implementation circumstances remain intricate and unstable. Correlated with the conventional wired network, this experiences several distinct issues and adversities. Initially, a solo SN's calculating potential and storage capacity remain considerably restricted, and the transmission capability betwixt the nodes remains frail. Additionally, the SNs will be frequently distributed at a large level or in an intricate or also in hard physical settings that turn it arduous or unattainable to execute maintenance jobs like energy supply. Furthermore, this remains an open network having vibrant and haphazard topology. Hence, it remains requisite to perform a sequence of target studies for assuring the live, energy-efficient, dependability, and the rest of the WSN's functioning necessities [8].

Being a data-centered network, several susceptible data will be gathered, stored, transferred, and processed within WSN. The security issue turned progressively crucial [9]. Because of WSN's constraints and attributes, the data will be effortless to be destructed, abducted, or altered. In what way to safeguard network security efficiently against diverse network attacks (NAs) remains a significant study matter. Regrettably, passive protection solely via firewalls, access control, and the rest remain inadequate in avoiding entire NAs.

Intrusion detection (ID) remains a preemptive safety feature technology, which could surveil the operational state of network systems and identify intrusions like internal attacks, external attacks, or dysfunctions, thereby this network system could intercept and reply as requisite [10]. Wired network ID technology remains fairly fully developed and could be split into 2 kinds – misuse-related and anomaly-related. The first kind's requisite remains that the attack methodology's knowledge is obtained, and the intrusion manner is determined beforehand. Intrusion will be identified by deciding in any case the gathered data features complement the intrusion pattern dataset. Hence, this just contains an elevated identification rate for particular attack methodologies and remains void for unfamiliar attacks. For coping with the diverse attacks' infinite occurrence, the second kind could be taken into consideration. This one presumes that cyber-attacks remain unusual when correlated with general conduct. By correlating the cached network conduct having general patterns, this could be decided in any case an intrusion has happened. This could address unforeseeable attacks, yet this requires learning numerous historical data for training [11].

For enhancing the identification efficacy, the AI's introduction remains anticipated. Several researchers attempted to imply artificial neural network (NN) [12], machine learning (ML), evolutionary computing [13], and so on into the ID discipline and attained productive study outcomes. Nevertheless, WSN possesses its self features and constraints concerning network scale, calculating potential, storage space, energy supply, transmission bandwidth, and networking mode that turns this unfeasible to straightly employ the conventional IDS framework. AI technology normally needs elevated calculating potential and utilizes fairly abundant running time, storage resources, and energy utilization. Hence, this remains requisite to do alterations and adaptations to the WSN ID paradigm as per the real implementation circumstances and user requisites and find the balance betwixt protection, energy utilization, actual time, and the rest of the targets. WSN ID, evidently, remains a technological issue having several limitations. In what way to give a possible and efficient resolution remains a vital problem that must be resolved imperatively. Several researchers performed constructive studies in this discipline [14].

Feature choosing remains a significant and pragmatic scheme for lightweight ID. Size lessening could enhance the ID's normalization execution and identification efficacy. The chief objective of an intrusion avoidance system remains in detecting the malevolent actions, and, later, it either identifies and permits or evades these malevolent actions. Fundamentally, in the ID and avoidance discipline, some works explored deep learning (DL), yet not any of these have victoriously employed the DL methodologies' complete potential [15]. Presently, DL has been majorly employed in several disciplines such as cyber security, speech detection, machine translation, and others [15]. By employing DL methodologies, we could enhance the efficacy and also accuracy rate of ID and avoidance within WSN. In DL, convolution NN (CNN) remains the majorly employed methodology. This study's inputs are as ensues:

The intrusion acts within the network will be identified by employing Cascaded Hermite Laguerra NN (CHLNNet) that embraces the data transition and acquire a fairly dependable trust value despite the data interchange.

Implementing multi-trusted Dempster-Shafter theory has unique and comprehensive feasibilities just like a state-space within the probability to improve the protection.

This study is organized as follows: Segment 1 mentions the ID's background WSNs and the function of deep NNs in ID, Segment 2 highlights the literature for secured and optimal routing in WSN, Segment 3 exhibits the proffered CHLNNet to seek the intrusions within the network, Segment 4 illustrates the experimental assessment provided with graphs by correlating the 3 conventional methodologies, and, lastly, Segment 5 sums up with a conclusion and prospective study.

2. RELATED WORKS

Lately, many IDS were proffered centered upon data mining, game theory, statistical methodology, immune theory, trust administration, and so on. Presently, a striking methodology is established to identify the atypical node by employing the trust-based system. In recent times, many studies have been published on trust-based IDS and its implementation.

Jiang et al. [16] present the ID methodologies for WSNs struggling with the drawbacks of less identification rate, huge computation overhead, and elevated false alarm rate because of the SNs' restricted resources, huge quantity of iteration, and also network data's elevated comparison. Concerning the aforementioned issues, the authors proffer SLGBM, an ID methodology for WSNs. Initially, the sequence backward selection (SBS) algorithm will be implemented for lessening the data size upon the initial traffic data's feature space for lessening the calculative overhead. A LightGBM algorithm will be later employed for identifying disparate NAs.

Wang et al. [17] discuss a vehicle collaboration sensing network paradigm in which the mobile sensing vehicles (MSV) and static SNs collaborate for giving ID opposing the empowered intruders (EIs). This paradigm, called IDEI, comprises a target pursuit algorithm of MSV and static nodes' (StN) sleep-management scheme. MSV would trace the EIs and complete the coverage breaches when the StN ensue a sleep-management procedure and would be woke by the neighboring identification nodes while the intruder remains identified.

Otoum et al. [18] present limited Boltzmann machine-based clustered IDS (RBC-IDS), a powerful DL-related IDS method to surveil crucial infrastructures by WSNs. The authors learned the RBC-IDS' execution and correlated this with the formerly proffered adaptive ML-related IDS: the adaptably administered and clustered hybrid IDS (ASCH-IDS).

Amaran and Mohan [19] propose Optimal Multilayer Perceptron (OMLP) alongside Dragonfly Algorithm (DA) for ID in WSN. OSVM's chief objective remains to decide the feasible intrusions and detect the class kind efficiently. This OMLP approach will be chiefly employed to discern the MLP's weights and bias by the DA. This DA's employment leads to the efficient selection of weight and bias values; so, this would pave the way to an enhanced identification execution.

Zhao et al. [20] examines and established DL-related network intrusion identification methodologies. Nevertheless, the DL's elevated calculative intricacy critically blocks the DL-related paradigm's real implementation, specifically in the WSN gadgets, which need not possess potential processing execution because of power constraints. The authors proffer a lightweight dynamic autoencoder network (LDAN) methodology for NID that recognize effectual feature extraction via a lightweight framework pattern.

Gil and Han [21] put forth a target centered upon a genetic algorithm (GA) coverage scheduling strategy employing evolutionary global search approaches for surveilling entire targets and could discover the optimal coverage set lengthening the network lifespan. Islam et al. [22] contemplate the employment of GA for enhancing the node positioning methodology that could attain the optimizing node coverage intention.

Shahbazi et al. [23] suggest an intelligent methodology centered upon Self Organizing Map (SOM) NNs, which augment the routing concerning every node's energy preservation and calculative power. Oldewurtel et al. [24] propose a SOM NN that is employed for lessening and classification of identical patterns (IP). The authors employ SOM in a stratified (cluster-related) network framework where the nodes remain as organizers in many clusters having a CH or merging centers. When lessening the data quantity to be transferred, the SOM executes clustering of IP.

Multiple elastic NN modules (MEMs) [25] remain an enhancement to SOM. MEMs normalize the self-organizing paradigm's parameters for facilitating the administration of high-level intricate optimization issues like computer vision. Automated context classification/detection, generally by the computing data assessment out of several SNs, remains a basic issue in human-computer communication.

Nevertheless, all the above algorithms possess a few constraints. The SOM NN's intricacy remains very elevated, and this can effortlessly result in the channel block while the communication data remains huge. The SBS algorithm's calculating intricacy and communication intricacy remain lesser, yet it has 2 issues: initially, incompetence for making the unnecessary nodes of surveillance region border still; next, it disregards the overlap betwixt node coverage regions that result in selected enormous functioning nodes, hence, impacting the network lifespan. Therefore, such restrains can be subdued by the proffered CHLNNet.

3. SYSTEM PARADIGM

WSN will be built in a homogeneous way in which the cluster will be created and the CH will be chosen. Figure 1 illustrates the system paradigm for secured and optimal data transmission (DT) in WSNs in which the intrusions will be identified by employing CHLNNet that, later, could assist in denying malicious nodes (MN). Next, the optimal route will be chosen.

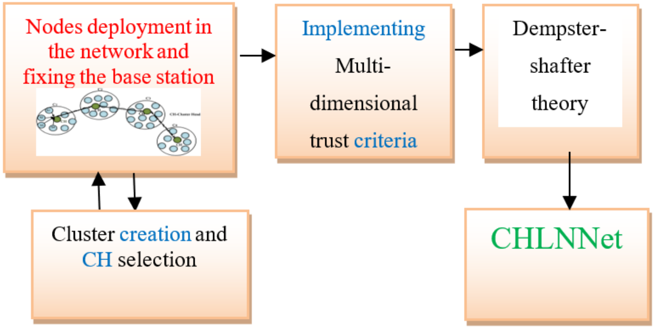
Nodes deployment in the network and fixing the base station
Implementing Multi-dimensional trust criteria
Dempster-shafter theory
Cluster creation and CH selection
CHLNNet

Figure 1. System paradigm for secured and optimal DT in WSN

4. CLUSTER FORMATION AND CH SELECTION (CHS)

CHS remains a tentative procedure having Energy-Based Timer (EBT) and Trust Value (TV) as illustrated in Figure 2. A node will be designated a timer for choosing Tentative CH (TCH), and TV will be computed centered upon the node's comprehensive TV. Nodes having the greatest TV and energy will be chosen as TCH. Additionally, the last CHS relies upon competing range, headcount, and node degree.

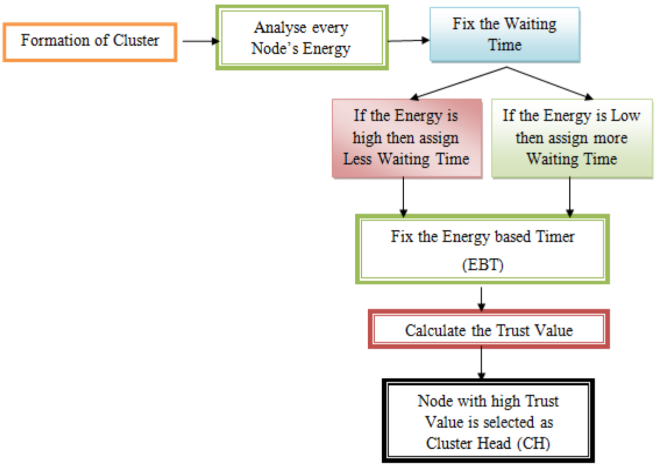
Formation of Cluster
Analyse every Node's Energy
Fix the Waiting Time
If the Energy is high then assign Less Waiting Time
If the Energy is Low then assign more Waiting Time
Fix the Energy based Timer (EBT)
Calculate the Trust Value
Node with high Trust Value is selected as Cluster Head (CH)

Figure 2. Block schematic illustration for CHS

5. TCH SELECTION CENTERED UPON EBT

Centered upon the energy of nodes (EoN) a timer will be designated to the nodes. The designated waiting time (WT) will be centered upon the EoN that ensues 2 circumstances – lesser WT will be designated to the greatest energy node (EN) and contrariwise. The node of which the timer value ends earliest will be selected as TCH. The node having the highest energy (HE) will be the subsequent TCH since the time designated to this remains lesser. Otherwise, the node with the HE for transference turns into CH. The timer centered upon energy will be defined as: Presume that there prevail k neighbors for node i, and for neighbor nodes (NbNs), the mean energy value can be computed by each node: Si={i_1, i_2, i_3, i_n….i_k} and i_n remains the *n*th NbN. The mean EoN i can be computed by:

$$Average\ Energy(i) = \begin{cases} \dfrac{1}{k}\displaystyle\sum_{n=1}^{k} Energy(i_n) & k > 0 \\ 0 & k = 0 \end{cases} \quad (1)$$

TCH would be chosen by employing an energy-related timer [19]. For whatsoever node having ID S_i, the WT centered upon energy can be computed by:

$$WaitTime\ (s_i) = \frac{AvgEnergyof\, s_i Neighbornode}{EnergyofS_i} \quad (2)$$

This remains apparent out of the above expression that WT lessens with the rise in EoN. The HE node will be mentioned to be TCH that sends messages in its range and the rest of the nodes relieve out of the CHS procedure when the message has been reached. TCH will be selected centered upon distance, total energy (E_{total}), and TV. Centered upon the TCH choosing procedure's criteria, the maximum and minimum node distance (ND) will be decided in each round. Distance means the number of edges between two nodes. The distance between nodes is the smallest number of edges from one node to the other. The node-node distance (NND) distribution depends on how the subsequent nodes are attached. If each node is connected with only one of the preexisting nodes (m=1) a tree appears.

6. TV-BASED TCH SELECTION

TV assists in identifying the node's conduct, quality, and, also, services. Furthermore, this will be incorporated in data collection, reconfiguration, routing, and, also, reinforces in analyzing the nodes' dependability. The TV performs a part in gathering data and observing diverse node events. TV alongside EBT will be employed to choose TCH for enhancing the finest CHS's efficacy. Nodes' TV can be calculated by:

$$Trust\ Value(TV)_{nodes} = \frac{N_{FD}}{N_{REC}} \tag{3}$$

where, N_{FD} and N_{REC} indicate the packets' quantity sent and obtained accordingly. TV for an independent node will be computed and the greatest TV node will be selected as TCH that will be ensued by the last CHS procedure, Lastly, TV and EBT give the TCH choosing procedure's result.

7. MULTIDIMENSIONAL TRUST CRITERIA

With the rate of the present node's straight communication with the sink node, the sink will be regarded as the base station (BS) of the adaptable network paradigm. The communication range for a sink remains the whole network. The node sends messages toward the sink. If the straight communication betwixt the node and sink remains higher, the contact value (CV) remains higher as depicted in the following expression:

$$Vc=\frac{Cs}{C} \tag{4}$$

where, Vc depicts the CV, Cs depicts the node's contact frequency (CF) with the sink, and C depicts the present node's CG with each network node (NtN) in the running time.

Location value (LV) remains the location degree association betwixt the node and sink. The portable gadget nodes act like a human. If the ND to the sink remains lesser, the node partly shifts toward the sink, the probability remains higher with the sink, and there remains a rise in the transfer probability as depicted in the following expression:

$$V_L=\frac{Cp}{Rp} \tag{5}$$

where, V_L denotes the LV, Cp denotes the packages' quantity forwarded by the node, and Rp denotes the packets obtained by the node out of the rest of the nodes.

8. DEMPSTER-SHAFTER (D-S) THEORY

D-S remains concerned regarding limits for probabilities of provability and not regarding assessing truth probabilities. In this, 2 bounds – belief (be) and plausibility (pl) – will be employed. Whatsoever hypothesis A indicates the proof subset provided by spectators. An array of each feasible subset of n including itself and the null set ∅ remains the power set (PS) indicated as 2^n. Thus, PS contains each feasible hypothesis or focal component 2^n={A_1, n, A_n}. Hypotheses could be designated to whatsoever 3 value kinds. Fundamental probability numbers called fundamental belief mass maps each hypothesis A to a value m(A) of which range remains from zero to one. Since some MN perform as usual NtN, calculating straight TV only remains incomplete. A part of TV called suggestion trust should be acquired out of the rest of the NtNs. Sum confidence value can be provided by:

$$T=T_{i,j}(\text{direct})+T_{i,j}(\text{recom}) \tag{6}$$

where, T denotes the total TV, i and j denote adaptable NtNs indicating the assessing node and node that is assessed accordingly, and $T_{i.j}$ (direct) and $T_{i.j}$ (recom) denote the direct TV and suggested TV of node i to j accordingly.

The direct TV can be calculated by:

$$\text{T(direct)}=\beta 1Vc+\beta 2VL \tag{7}$$

where, 1 and 2 portray the weight coefficients of CV and LV accordingly that influence the system. Such values modify after a while and differ with node object named correlation. The Grey Association assessment approach that employs a gray correlation degree will be employed for assessing and deciding the system's influence or calculating the system's apportionment. The algorithm will be implemented with diverse capabilities, inconsistent samples requiring just some computations, and lesser time intricacy.

9. CHOOSING OPTIMAL ROUTE AND INTRUSION CLASSIFICATION EMPLOYING CHLNNET

The power utilized by the SNs differs with the settings positioned. In the route building stage, the optimal least route will be discerned that remains employed for DT. For transferring each data bit, the network will be conscious of the energy level. Each NtN obtains DREQ (data request) out of the BS, and, later, replies with DREP (data reply). When the DREQ has been obtained, a few processes have ensued. The node with the unique shared key (SK) will approve the message, and if it is complimented, the packet will get acknowledgement. The node will use the SK throughout to link with the BS. The data will not be transmitted if the sources and destinations stay on the same node. The best path will be chosen by the BS based on the earlier phase, whenever data are collected from each NtN, and then the route request will be transmitted. The node will accept the message and transmit an error packet (ERRP) only when DREP as well as SK are complemented. CHLNNet functions appertain to the orthonormal functions' (OF) normal class. This is centered upon activation functions in the hidden layer employing the result of a Hermite polynomial (HP) $H_n(t)$ and a Gaussian function t as in the following expression:

$$h_n(t) = \frac{H_n(t)}{\sqrt{2^n n\sqrt{\pi}}} \exp\left(\frac{-t^2}{2}\right) \tag{8}$$

where, the initial HP $H_0(t)$=1 and the rest of polynomials (n≥1) 1/ will be centered upon the recurrence associations.

$$H_n(t) = 2tH_n(t) - 2nH_{n-1}(t) \tag{9}$$

The Hermite activation functions (AF) for n=1, 2, …., 10. First-order derivatives for this AF remain:

$$\frac{dh_n\,(t)}{dt} = \sqrt{2nh_{n-1}}(t) - th_n\,(t) \quad n \geq 1 \tag{10}$$

$$\frac{dh_0\,(t)}{dt} = -th_0\,(t) \quad n = 0 \tag{11}$$

The rate can be decided for a rising hidden units' (HUs) quantity n=1, 2, …., 10 in which $h_n(t)$ and $H_n(t)$ are computed for the nth HU with $t = \sum_j w_{jn,}\, x_{ij}$ for the nth rface HU and ith input sample containing j features. MSE values as a function of the hidden nodes' quantity n are computed for ten-fold cross authentication employing fifty sweeps for every fold. Earlier weight values upon the input side are fixed to haphazardly sampled count out of the standard normal dispensation when output-side (OS) weights are initialized in the range [-0.5,0.5]. Furthermore, for the HNN, the OS AF remains the softmax.

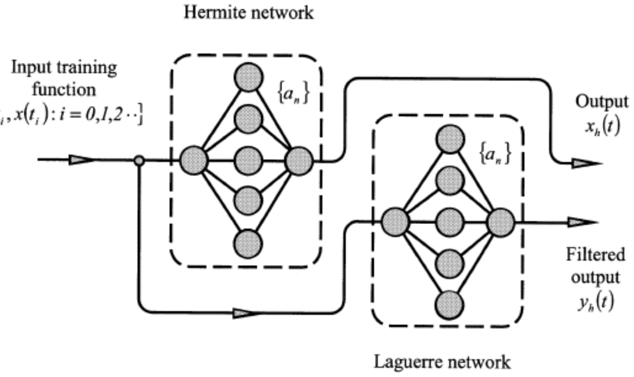

Figure 3. CHLNNet framework for classification

This comprises 2 networks – the Hermite network (HN) and the Laguerre network (LN) as shown in Figure 3. The initial output will be out of the HN, and the next will be out of LN that calculates the noisy function's (NF) correlation with the filter function. The network will be trained by lessening the error betwixt the HN and the training data (TD) out of the NF. The trained HN's weights will be forwarded straightly to the LN.

10. TRAINING PROCEDURE

As the LN's weights will be forwarded to it out of the HN, just the second network requires to be trained. A parameter frequently implemented for determining the NNs' error remains the root mean square error (RMSE) that is provided as:

$$\text{rmse} = \sqrt{\frac{\int_{+\infty}^{-\infty}\left(\mathrm{x(t)} - x_h(t)\right)^2 dt}{N}} \tag{12}$$

The benefit of employing OF as AF correlated to sigmoidal functions remains the simplicity and speed wherewith the optimal weights (OW) could be computed. This might be displayed that, for OF, this error remains minimal if the weights will be provided by the integration:

$$a_m = \int_{-\infty}^{+\infty} x(t)h_m\,(t)dt \tag{13}$$

For training the Hermite orthonormal network, this integral has been estimated arithmetically by the TD $\{x(t_i): i = 0,1,2\,\ldots.I\}$ on the interval $\frac{-T}{2} \leq t \leq \frac{T}{2}$:

$$a_m = \frac{T}{I} \leq x(t_i)h_m\,(t_i) \tag{14}$$

where, I portrays the TD's sum quantity. The OW could be later acquired by implementing the gradient descent algorithm upon the error $E(ti)$ betwixt the TD and NN interpolation.

$$a_m(t_{i+1}) = a_m(t_i) - \tau\frac{de(t_i)}{da_m} \tag{15}$$

where, τ portrays the learning rate coefficient determined by the number of attempts, and the error $e(t_i)$ remains.

$$e(t_i) = \left(x(t_i) - \sum_{n=0}^{N} a_n\,h_n\,(t_i)\right) \tag{16}$$

Even though there remain much numerical integration's intricate methodologies, the summation's benefit will be as well implemented to haphazardly dispensed data; in such format, this calculates the Monte-Carlo integration. For approximating a function, the required network's dimension should be analyzed and the training function scaled into the network's suitable range. Such features will be decided out of the network's spatial and frequency bandwidth (SFB). Effectual function approximation incorporates complementing the network's SFB as near as feasible to that of the function. Because of the Hermite function's (HF) augmented decay, the functions' effectual range will be remarkably below the orthonormal situation's infinite internal. For interpolation intentions, just the HF's middle part that looks like a cosine remains effectual. In the network, the highest-order HF's middle area remains:

$$t_B = \pm\sqrt{2n+1} \tag{17}$$

where, n represents the HF's order. A methodology for bypassing this remains to cascade a sequence of m=0, 1, 2…. M similar NN modules alongside the data range by transferring every network's origin. Multi-dimensional trust criteria will be used to determine the cluster pathways' (CP) optimal range for effective data transfer, with residual energy and distance being the key constraints Avg portrays the mean packet dimension in calculating Throughput of the network. Packet dimension is one of the main criteria for evaluating the performance analysis of the network. In such a manner, an agreeably little window could be attained. Every independent Hermite/Laguerre (H/L) NN module presently needs a bias β_m and an output-processing element's (OPE) transfer function (TF) $\emptyset\ (t)$ provided as:

$$\beta_m = 10m \tag{18}$$

and

$$\emptyset\ (t) = \begin{cases} 1, for\ -5.0 \leq t \leq 5.0 \\ 0\ for\ t > 5.0 \\ 0\ for\ t < -5.0 \end{cases} \tag{19}$$

The OPE's TF limits every independent H/L NN module's output signal, thereby this in no way intrudes with the nearby modules. The HLCNNet outputs will be provided by:

$$x_h(t) = \sum_{m=0}^{M} \sum_{n=0}^{N} a_{mn} \emptyset\ (t - \beta_m)\ h_n\ (t - \beta_m) \tag{20}$$

11. PERFORMANCE ANALYSIS

The experimental result has been performed by employing the criteria employed for assessing routing overhead, end-to-end delay, throughput, average latency, ID rate, and packet delivery ratio. Such criteria will be correlated with 3 conventional techniques - restricted Boltzmann machine-based clustered IDS (RBC-IDS), Optimal Multilayer Perceptron (OMLP) with Dragonfly Algorithm (DA) called (OMLP-DA), and Multiple elastic neural network modules (MEMs) with the proffered CHLNNet. The following Table 1 exhibits the simulation setup.

Table 1. Simulation setup

Criteria	Values
No. of normal nodes	500
No. of MN	100
No. of sink	1
Simulation region	1000*1000 m
Packet dimension	300KB
Transmission rate	200KB
Communication range	30m

Routing overhead (RO) might be regarded as the routing packets' (RP) number forwarded for upkeep and so well for route invention that is provided in the following expression:

$$\text{RO}=\frac{H}{P} \tag{21}$$

where, *H* will be calculated once per hop, and *P* remains the sum of RP.

Table 2 exhibits the RO's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology.

Figure 4 illustrates RO's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology in which the X-axis represents the MN's quantity employed for assessment, and the Y-axis represents the RO values acquired in percentage. While correlated, the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies attain 45.2%, 40.2%, and 35.4% whereas the proffered CHLNNet methodology attains 31.4% that remains 13.8% finer than RBC-IDS, 8.8% finer than OMLP-DA, and 4% finer than MEMs.

Table 2. RO's correlation

No. of MN	RBC-IDS	OMLP-DA	MEMs	CHLNNet
20	38	35	31	25
40	42	38	34	28
60	45	41	36	32
80	49	42	37	35
100	52	45	39	37

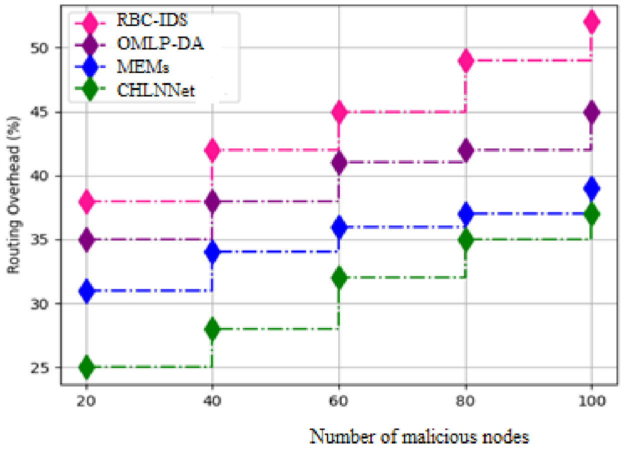

Figure 4. RO's correlation

End-to-end delay (E2ED) refers to the time consumed for packet transmission out of the source toward a network's sink.

Table 3 exhibits the E2ED's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology.

Table 3. E2ED's correlation

No. of MN	RBC-IDS	OMLP-DA	MEMs	CHLNNet
20	39	32	25	16
40	42	35	29	19
60	45	39	32	22
80	49	42	35	26
100	51	46	39	32

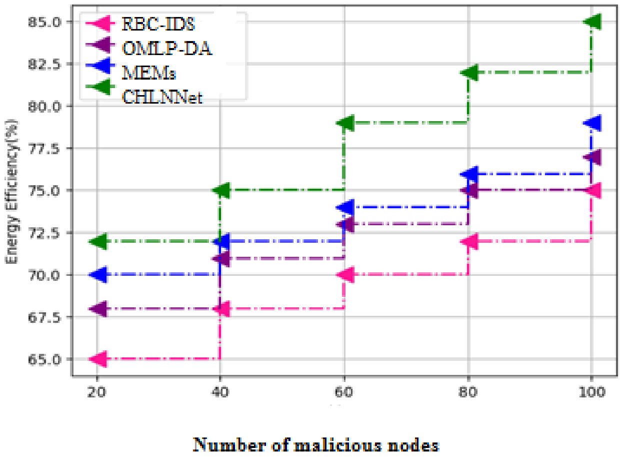

Figure 5. EE's correlation

Figure 5 illustrates EE's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology in which the X-axis represents the MN's quantity employed for assessment, and the Y-axis represents the EE values acquired in percentage. While correlated, the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies attain 70%, 72.8%, and 74.2% whereas the proffered CHLNNet methodology attains 78.6% that remains 8.6% finer than RBC-IDS, 6.2% finer than OMLP-DA, and 4.2% finer than MEMs.

Throughput (TP) refers to the DF via a channel employed for communication, that is, bits or packets supplied victoriously above a channel within the network. In WSN-IoT implementations, Tp remains substantially significant that is provided in the following expression:

$$\text{Throughput (bits/sec)}=\sum \frac{\mathbf{(n)*(avg)}}{\mathbf{T}} \qquad (23)$$

where, *n* portrays victorious packets' quantity, Avg portrays the mean packet dimension, and T portrays the total time spent in delivering the data.

Table 4 exhibits the TP's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology.

Table 4. TP's correlation

No. of MN	RBC-IDS	OMLP-DA	MEMs	CHLNNet
20	83	85	90	92
40	84	86	91	93
60	86	88	93	95
80	88	90	94	96
100	90	92	95	98

Figure 6 illustrates TP's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology in which the X-axis represents the MN's quantity employed for assessment, and the Y-axis represents the TP values acquired in percentage. While correlated, the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies attain 86.2%, 88.2%, and 92.6% whereas the proffered CHLNNet methodology attains 94.8% that remains 8.6% finer than RBC-IDS, 6.6% finer than OMLP-DA, and 2.2% finer than MEMs.

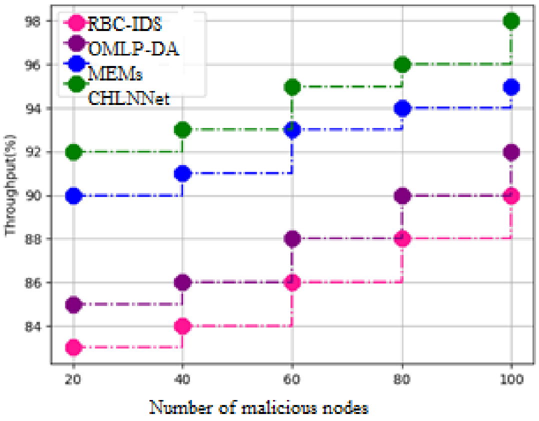

Figure 6. TP's correlation

Average latency (AL) could be computed betwixt the packets that rely upon the present position as to sink. For a packet while doing the transfer, the anticipated delivering packet's latency via the allotted path P_{mn} will be provided as exhibited in the following expression:

$$P_{mn=}p_{mn+}\sum_{jN(n)}(Pnj \times Dnj) \qquad (24)$$

where, P_{mn} indicates the data delivery delay, *Pnj* indicates the probability which the packet will be sent via the allotted path, N(n) indicates the nearby channel's quantity, and *Dnj* indicates the distance betwixt both the paths.

Table 5 exhibits the AL's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology.

Table 5. AL's correlation

No. of MN	RBC-IDS	OMLP-DA	MEMs	CHLNNet
20	38	34	31	24
40	40	35	34	26
60	45	39	36	29
80	49	42	39	30
100	50	45	42	32

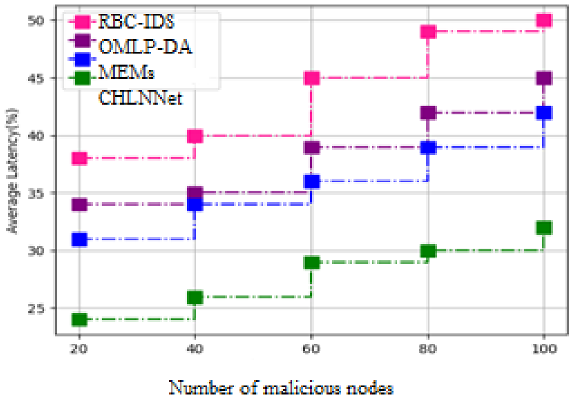

Figure 7. AL's correlation

Figure 7 illustrates AL's correlation betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology in which the X-axis represents the MN's quantity employed for assessment, and the Y-axis represents the AL values acquired in percentage. While correlated, the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies attain 44.4%, 39%, and 36.4% whereas the proffered CHLNNet methodology attains 28.2% that remains 16.2% finer than RBC-IDS, 10.8% finer than OMLP-DA, and 8.2% finer than MEMs.

Table 6 exhibits the comprehensive correlative assessment betwixt the prevailing RBC-IDS, OMLP-DA, and MEMs methodologies and the proffered CHLNNet methodology.

Table 6. Comprehensive correlative assessment

Criteria	RBC-IDS	OMLP-DA	MEMs	CHLNNet
RO (%)	45.2	40.2	35.4	31.4
E2ED (%)	45.2	38.8	32	23
EE (%)	70	72.8	74.2	78.6
TP (%)	86.2	88.2	92.6	94.8
AL (%)	44.4	39	36.4	28.2
Malicious Detection Rate – MDR (%)	80.8	84.6	88	91.4

12. CONCLUSIONS

WSNs swiftly reply to malevolent attacks, specifically in armed forces that remain more susceptible field. Hence, the present study presents a new routing technique named CHLNNet for protecting from attacks and as well give the least path for transmitting packets. Out of the outcomes attained, this confirms that the CHLNNet methodology assures 31.4% RO, 23% of E2ED, 78.6% of EE, 94.8% of TP, 28.2% of AL, and 91.4% of MDR. Hence, the outcome exhibits that the proffered paradigm remains very effectual and greatly dependable while correlated with the prevailing techniques. In the prospective study, this methodology could be optimized and depth assessment could be done by employing disparate attacks such as sleep deprivation and directional antenna that provides denial of service.

REFERENCES

[1] Ishmanov, F., Malik, A.S., Kim, S.W., Begalov, B. (2015). Trust management system in wireless sensor networks: Design considerations and research challenges. Transactions on Emerging Telecommunications Technologies, 26(2): 107-130. https://doi.org/10.1002/ett.2674

[2] Syed, M., Dubey, M.K. (2020). Software-Fault mitigation for derivation of quality of services (QoS) in wireless sensor networks (WSN). Instrumentation, Mesures, Métrologies, 19(5): 327-336. https://doi.org/10.18280/i2m.190502

[3] Phijik, B., Rao, C.V.G. (2021). Pragmatic security-aware cross-layer design for wireless networks from vampire attacks. Ingénierie des Systèmes d'Information, 26(6): 559-567. https://doi.org/10.18280/isi.260606

[4] Liu, Y., Dong, M., Ota, K., Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9): 2013-2027. https://doi.org/10.1109/TIFS.2016.2570740

[5] Atayero, A.A., Ilori, S.A., Adedokun, M.O. (2015). Development of FIGA: a novel trust-based algorithm for securing autonomous interactions in WSN. In Accepted, International Conference on Computer Science Applications (ICCSA), pp. 174-180.

[6] Gavel, S., Raghuvanshi, A.S., Tiwari, S. (2021). A novel density estimation based intrusion detection technique with Pearson's divergence for wireless sensor networks. ISA Transactions, 111: 180-191. https://doi.org/10.1016/j.isatra.2020.11.016

[7] Han, L., Zhou, M., Jia, W., Dalil, Z., Xu, X. (2019). Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model. Information Sciences, 476: 491-504. https://doi.org/10.1016/j.ins.2018.06.017

[8] Çalışır, S., Atay, R., Pehlivanoğlu, M.K., Duru, N. (2019). Intrusion detection using machine learning and deep learning techniques. In 2019 4th International Conference on Computer Science and Engineering (UBMK), Samsun, Turkey, pp. 656-660. https://doi.org/10.1109/UBMK.2019.8906997

[9] Gulla, K.K., Viswanath, P., Veluru, S.B., Kumar, R.R. (2020). Machine learning based intrusion detection techniques. In Handbook of Computer Networks and Cyber Security, pp. 873-888. https://doi.org/10.1007/978-3-030-22277-2_35

[10] Osken, S., Yildirim, E.N., Karatas, G., Cuhaci, L. (2019). Intrusion detection systems with deep learning: A systematic mapping study. In 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), pp. 1-4. https://doi.org/10.1109/EBBT.2019.8742081

[11] Chai, Q. W., Chu, S. C., Pan, J. S., & Zheng, W. M. (2020). Applying Adaptive and Self Assessment Fish Migration Optimization on Localization of Wireless Sensor Network on 3-D Te rrain. Journal of Information Hiding and Multimedia Signal Processing, 11(2): 90-102.

[12] Zarpelão, B.B., Miani, R.S., Kawakani, C.T., de Alvarenga, S.C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84: 25-37. https://doi.org/10.1016/j.jnca.2017.02.009

[13] Ma, T., Wang, F., Cheng, J., Yu, Y., Chen, X. (2016). A hybrid spectral clustering and deep neural network ensemble algorithm for intrusion detection in sensor networks. Sensors, 16(10): 1701. https://doi.org/10.3390/s16101701

[14] 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. https://doi.org/10.1109/ACCESS.2017.2762418

[15] Xue, Y., Jia, W., Zhao, X., Pang, W. (2018). An evolutionary computation based feature selection method for intrusion detection. Security and Communication Networks, 2018: 2492956.

[16] Jiang, S., Zhao, J., Xu, X. (2020). SLGBM: An intrusion detection mechanism for wireless sensor networks in smart environments. IEEE Access, 8: 169548-169558. https://doi.org/10.1109/ACCESS.2020.3024219

[17] Wang, W., Huang, H., Li, Q., He, F., Sha, C. (2020). Generalized intrusion detection mechanism for empowered intruders in wireless sensor networks. IEEE Access, 8: 25170-25183. https://doi.org/10.1109/ACCESS.2020.2970973

[18] Otoum, S., Kantarci, B., Mouftah, H.T. (2019). On the feasibility of deep learning in sensor network intrusion detection. IEEE Networking Letters, 1(2): 68-71. https://doi.org/10.1109/LNET.2019.2901792

[19] Amaran, S., Mohan, R.M. (2021). An optimal multilayer perceptron with dragonfly algorithm for intrusion detection in wireless sensor networks. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC), pp. 1-5. https://doi.org/10.1109/ICCMC51019.2021.9418355

[20] Zhao, R., Yin, J., Xue, Z., Gui, G., Adebisi, B., Ohtsuki, T., ... & Sari, H. (2021). An efficient intrusion detection method based on dynamic autoencoder. IEEE Wireless Communications Letters, 10(8): 1707-1711. https://doi.org/10.1109/LWC.2021.3077946

[21] Gil, J.M., Han, Y.H. (2011). A target coverage scheduling scheme based on genetic algorithms in directional sensor networks. Sensors, 11(2): 1888-1906. https://doi.org/10.3390/s11020188

[22] Islam, M., Ahasanuzzaman, M., Razzaque, M., Hassan, M.M., Alelaiwi, A., Xiang, Y. (2015). Target coverage through distributed clustering in directional sensor networks. EURASIP Journal on Wireless Communications and Networking, 2015(1): 1-18.

https://doi.org/10.1186/s13638-015-0394-2

[23] Shahbazi, H., Araghizadeh, M.A., Dalvi, M. (2008). Minimum power intelligent routing in wireless sensors networks using self organizing neural networks. In 2008 International Symposium on Telecommunications, pp. 354-358. https://doi.org/10.1109/ISTEL.2008.4651327

[24] Oldewurtel, F., Mahonen, P. (2006). Neural wireless sensor networks. In 2006 International Conference on Systems and Networks Communications (ICSNC'06), pp. 28-28. https://doi.org/10.1109/ICSNC.2006.56

[25] Liu, M., Li, H., Shen, Y., Fan, J., Huang, S. (2009). Elastic neural network method for multi-target tracking task allocation in wireless sensor network. Computers & Mathematics with Applications, 57(11-12): 1822-1828. https://doi.org/10.1016/j.camwa.2008.10.050