

Optimized Dual Temporal Gated Multi-Graph Convolution Network for Land Use and Land Cover Classification Incorporating Temporal Feature Tracking and High Resolution Satellite Imagery Analysis

Kamalakkannan D

drkamalakannand@gmail.com

Anna University

Parul Awasthi

Chhatrapati Shahu Ji Maharaj University

Shaman Bhat

Pediatric Endocrine Society

Monali Shetty

Fr. Conceicao Rodrigues College of Engineering

Research Article

Keywords: Forward Private Verifiable Dynamic Searchable Symmetric Encryption, Humboldt Squid Optimization Algorithm, Lotus Effect Optimization, Spatial Bayesian Neural Network, and Triple-Memristor Hopfield Neural Network

Posted Date: August 24th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10466288/v1>

License:  This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Optimized Dual Temporal Gated Multi-Graph Convolution Network for Land Use and Land Cover Classification Incorporating Temporal Feature Tracking and High Resolution Satellite Imagery Analysis

**Dr. Kamalakkannan D.^{1*}, Mrs. Parul Awasthi², Mr. Shaman Bhat³, Mrs. Monali
Shetty⁴**

^{1*}Professor, Biomedical Engineering, Anna University, Tamil Nadu, India

^{1*}Email: drkamalakannand@gmail.com

*²Assistant Professor, Electronics Communication & Engineering, School of Engineering &
Technology (UIET) Chhatrapati Shahu Ji Maharaj University, Kanpur, Uttar Pradesh, India*

*³Software Engineer, Cisco Meraki,
San Francisco, California, United States*

*⁴Assistant Professor, Department of Computer Science Engineering, Fr. Conceicao
Rodrigues College of Engineering, Bandra, Mumbai, India*

Abstract

The dynamic nature of data transfer has led to its increasing appeal in Wireless Sensor Network (WSN) contexts. The WSN encounter various difficulties when transmitting data, like reduced energy efficiency, more severe security, shorter network lifetime. This work addresses these issues by presenting secure and energy-efficient routing and clustering techniques for an edge-assisted WSN environment. In this manuscript, Secure-Multipath Routing using Optimized Triple-Memristor Hopfield Neural Network with Block chain for Edge-Assisted WSN Environment (SMR-OTMHNN-WSN) is proposed. This work creates a network using a Spatial Bayesian Neural Network (SBNN) to improve the network management performance while decreasing complexity. The sensors are authenticated using

the Forward Private Verifiable Dynamic Searchable Symmetric Encryption (FPVDSSE) to eliminate fraudulent nodes and ensure high security after network construction. The node formation performed in edge server, the node are clustered by merging or combining two maximum comparable cluster nodes; then cluster head selection using Humboldt Squid Optimization Algorithm (HSOA) depending upon the parameters like Trust (T), Energy (E), Distance (Dist), Delay (D), Direction and Node Connectivity. Sensor nodes (SN) continuously transmit data; the system uses Twin Actor Twin Delayed Deep Deterministic policy gradient (TATD3) based duty cycling to save energy by allocating time slots to each sensor. The experimental outcomes of proposed SMR-OTMHNN-WSN method attains 14.25%, 21.25%, and 18.27% lower energy consumption; attains 19.79%, 27.41% and 24.94% higher Network Lifetime, and attains 18.79%, 25.41% and 26.94% greater Packet Delivery Ratio with existing techniques like “Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning based Routing using Block chain for Edge Assisted WSN Environment (SEE-DL-WSN)”, “Automata based hybrid PSO–GWO algorithm for secured energy efficient optimal routing in wireless sensor network (PSO-GWO-SEE-WSN)” and “Energy-efficient and delay sensitive routing paths using mobility prediction in mobile WSN: mathematical optimization, Markov chains, and deep learning approaches (EE-WSN-MC-DL)” respectively.

Keywords: *Forward Private Verifiable Dynamic Searchable Symmetric Encryption, Humboldt Squid Optimization Algorithm, Lotus Effect Optimization, Spatial Bayesian Neural Network, and Triple-Memristor Hopfield Neural Network.*

Introduction

The elements of WSN, which track and record environmental variables including vibration, motion, and temperature in real time, are distributed sensor nodes and one or more sink nodes [1]. Numerous uses for a WSN exist, such as air quality monitoring, crop monitoring, and forest fire detection [2]. However, network lifetime and delay are the two critical WSN

characteristics that is resolved through the use of clustering, duty cycling, and routing [3]. Random deployment requires a lot of energy due to the complexity of maintaining sensor nodes [4]. The sensor nodes are therefore best positioned in grid-based, hexagonal, and zone-based topologies [5]. Clustering is the most important WSN methods that reduce energy usage since it can collect sensed data from several nodes rather than just one [6]. Using bio-inspired optimization techniques; the best Cluster Head (CH) is selected during the clustering process [7]. When the optimal CH selection results in outstanding communication efficiency and reliability, network lifetime is increased [8]. Duty cycling represents yet another essential WSN function for energy efficiency, as it schedules the SN and assigns a time window to every sensor [9]. Sensor nodes have the option to be scheduled in ON, OFF, or IDLE states, which can increase the network's longevity. The proposed method distributes sensing actions according on the time allotted to them [10]. By disabling a sensor node, this technique reduces energy consumption without affecting the system's overall functionality. Recently, a deep learning approach to node scheduling was presented [11], which minimizes reward functions to generate optimal scheduling strategies. Maximizing the energy in SN to extend network lifetime is one of the main problems in WSN, and it can be addressed by creating an energy-efficient routing algorithm [12]. Routing data packets across many hops is necessary for nodes that are typically far from the source and destination due to coverage and distance concerns. Sensitive data from cluster head is transferred to sink or base station (BS) via routing in WSN [13]. The best route is selected from a range of possibilities in order to minimize routing failure brought on by excessive delay. Data is sent via the quickest and most efficient multi-hop routing path when using a cluster-based routing protocol. The nodes can keep an eye out for malicious activities within the WSNs thanks to multi-hop routing. The most urgent problem in WSNs is establishing safe routing protocols because of the existence of hostile nodes [14]. Vulnerable attacks on numerous nodes by attackers turn

WSNs into insecure settings. Sensitive data from CH is transferred to the BS or sink via routing in WSN. In order to minimize routing failure brought on by high latency, the best route is chosen among multiple options [15].

The problems with previous work uses metaheuristic optimization techniques for routing, this resulted in slower convergence. Random sensor node placement increases complexity and reduces network administration capacity. Routing is often utilized without scheduling, resulting in high energy use. Inadequate CH selection might result in substantial packet loss due to restricted parameters used in previous studies. Safe routing, attackers can readily imitations data owing to lack of security [16-22].

The motivation for addressing these issues is clear: improving routing efficiency, reliability, and security in wireless sensor networks is critical for successful deployment and operation in various applications. By developing more robust and efficient routing algorithms, it can improve network performance, reduce energy consumption, reduce packet loss, and strengthen security measures to protect against potential threats. Addressing these issues will result in more dependable and secure wireless sensor networks that can effectively support various applications across multiple industries.

The use of SBNN for network management represents a new method for increasing efficiency and decreasing complexity in WSN. SBNN reduces energy consumption, increase network performance, and reduce data collisions by incorporating dynamic clustering it enables the creation of efficient clusters that can help reduce energy consumption by grouping sensors based on various criteria, prioritization, TATD3-based duty cycling, and Secure Multipath Routing with TMHNN in Multi-Access Edge Computing IoT Sensor Networks. The proposed TMHNN architecture now incorporates LEOA for parameter optimization. This novel technique enables more effective and efficient network management, improving overall performance and reliability in WSN.

The main concept of the research is given below:

- The proposed SMR-OTMHNN-WSN work uses a SBNN structure to build the network, improve network management efficiency, and decrease complexity.
- Following network construction, sensors are authenticated based on their ID and location using the FPVDSSE, which successfully eliminates unauthorized sensor nodes while maintaining high security.
- The proposed SMR-OTMHNN-WSN model employs HSOA to cluster data and select the best CH. Dynamic selection and clustering of CHs based on time as well as event metrics improve communication efficacy and reduce energy consumption.
- The proposed SMR-OTMHNN-WSN technique performs duty cycling with TATD3 algorithm, increasing the network lifetime for reducing energy consumption.
- Finally, a safe multiple path routing is performed with a Triple-Memristor Hopfield Neural Network (TMHNN). During routing, TMHNN ranks the chosen multiple paths depending upon hop counts.

The remaining manuscript arranged as: segment 2 presents literature review, segment 3 describes the proposed approach, the outcomes and discussion is illustrated in segment 4, conclusion is presented in segment 5.

2. Literature Review

Numerous researches based on Energy-Efficient Routing for IoT-Based WSN Environment is suggested, some of recent research works are deliberated here,

Prasad and Periyasamy[16] have presented block chain technology for deep learning-based routing and secure, energy-efficient bio-inspired clustering in an edge-assisted WSN. The presented study builds a network using a quad-tree structure and uses the Lightweight Encryption Algorithm to authenticate sensors. The presented study employs the Tasmanian Devil Optimization to select the optimal CH and Improved Twin Delayed Deep Deterministic

Policy Gradient algorithm for duty cycling. Finally, a Generative Adversarial Network was used to ensure secure multipath routing. It provides high throughput and low Network Lifetime.

Prithiand Sumathi [17] have presented a hybrid PSO–GWO algorithm based on automata for safe, effective, and optimal routing in WSN. The goal of this effort is to send data securely across an upgraded path while utilizing energy as little as possible. To grasp the environment's dynamic role, a Learning Dynamic Deterministic Finite Automata (LD2 FA) was created. For route optimization, LD2 FA gives hybrid PSO-GGWO learned and accepted strings. It provides high Network Lifetime and high energy consumption.

Montoya et al., [18] have presented mobility prediction in mobile WSN to present energy-effective and delay-sensitive routing paths employing deep learning, Markov chains, and mathematical optimization. In order to determine the shortest communication path among a source node and sink while using the least amount of energy, this work presents a predictive distributed routing approach depending upon Markov Chains that takes network mobility. Additionally, it offers a deep learning strategy for projecting node distances in the future inside a mobile network. It provides Packet Delivery Ratio and low alive nodes.

Sharma and Kansal [19] have presented Advanced ANN based secured energy effectual routing protocol in WSN. In the presented paper, an advanced Low-Energy Adaptive Clustering Hierarchy was employed to efficiently select cluster heads (CH) based on energy. Furthermore, an optimized routing protocol depending upon the grasshopper optimization algorithm (GOA) was utilized to ensure shortest path transmission with lesser energy consumption. The presented Optimized Artificial Neural Network achieves a safe and energy effective shortest path for data transmission. It provides low energy consumption and high latency.

Gurram et al., [20] have presented Secure Energy Aware Meta-Heuristic Routing Protocol (SEAMHR) for IoT wireless sensor networks (WSNs) that strive to be sustainable. The presented paper introduced the SEAMHR (Secure Energy-Aware Meta-Heuristic Routing) protocol for WSNs with the intention of improving network security and performance. The recommended approach starts with Meta-Heuristic analysis based on MEHO (Mutation Elephant Herding Optimization) in order to obtain reliable and intelligent learning. It provides high alive nodes and low throughput.

Dineshand Svn [21] have presented GWO-SMSLO, a secure modified Sea Lion optimization routing technique for clustering based on Grey Wolf optimization, in wireless sensor networks. This work uses modified Sea Lion Optimization (SLO) for efficient routing and Grey Wolf Optimization (GWO) for effective node clustering. Elliptic Curve Cryptography, which uses a certificate-less aggregate signature system that provides conditional privacy, ensures the security of provided scheme. It provides low latency and low Packet Delivery Ratio.

Gulganwaand Jain [22] have presented the EES-WCA, a machine learning approach to safe and energy-effectual weighted clustering for WSN. The presented method doesn't interfere with the regular operations of the WSN; instead, it first establishes network clusters before gathering traffic samples on the BS. The BS classifies traffic data and finds malevolent nodes in the network using two machine learning techniques: Multi-Layer Perceptron and Support Vector Machine. It provides greater Network Lifetime and high energy consumption.

3. Proposed methodology

In the section, the SMR-OTMHNN-WSN methodology is proposed using deeplearning-based energy-effectual routing for an IoT-based WSN environment. It comprises of four processes, likes network setup, authentication, clustering, duty Cycling, path selection, node

optimization. Network coverage, connection, and lifespan are used in selecting the clustering heads. The HSOA is utilized to choose the ideal routing path after deciding on the best CH. The Triple-Memristor Hopfield Neural Network was utilized to ascertain the ideal routing path once the best CH is chosen. Consequently, a full explanation of each stage is provided below. Block diagram of proposed SMR-OTMHNN-WSN for secure multipath routing in WSN environment is presented in figure 1.

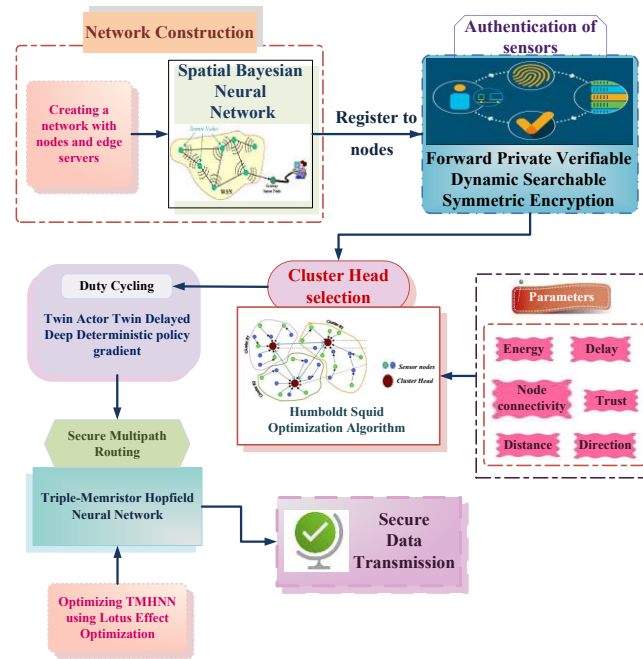


Figure 1: Block diagram of the proposed SMR-OTMHNN-WSN Architecture

3.1 Proposed Model

This proposed model utilized blockchain technology for safe clustering and routing in wireless sensor network settings. This proposed model aims to increase throughput and security while decreasing latency and energy usage. Sensor nodes, cloud servers, blockchains, and edge servers (including scheduling, clustering, and routing agents) are all covered under this approach. The six main procedures that are used to carry out this work are mentioned below.

- Spatial Bayesian Neural Network-based Network Construction

- Authentication of sensors using Forward Private Verifiable Dynamic Searchable Symmetric Encryption
- Energy Efficient Clustering with HSOA is used for Cluster Head selection.
- Duty Cycling using Twin Actor Twin Delayed Deep Deterministic policy gradient
- Secure Multipath Routing using Triple-Memristor Hopfield Neural Network
- Optimization using Lotus Effect Optimization

The proposed work's entity descriptions are listed below:

- Sensor nodes:** Sensor nodes monitor and update the status of wireless sensor network environment.
- Edge Server:** This provides additional resources to the WSN, minimizing energy consumption and latency. The system comprises 3 agents of clustering, scheduling, and routing, resulting in a longer network lifetime.
- Cloud Server:** Updates and stores sensor node data for future use, reducing storage requirements in the WSN environment.
- Blockchain:** A tamper-proof ledger is used to secure the WSN environment by storing transactions like authentication, clustering, scheduling, routing, encrypted data. This leads to increased safety and lower packet loss rates.

Radio Model for Communication:

The First-Order radio technique simplifies communication behavior in WSN. It shows the energy consumption as well as transmission range of devices. This includes models like

Transmit Energy (F_{tr}): This is the amount of energy utilized by a node when transmitting the data over specific distance. It increases the energy depending upon distance to receiver.

- **Receiver Energy (F_{re}):** It is this energy that a node needs to get data from another node.

The distance between the sender and the destination determines, like it does the transmitter. The first-order radio approach measures the energy used by a sensor node in

relation to the distance traveled at each transmission or reception cycle. The energy needed to send or obtain a packet over 'e' is expressed in equations (1) & (2).

$$F_{tr} = l * e \quad (1)$$

$$F_{te} = l * e \quad (2)$$

Where, F_{tr} indicates the, F_{te} signifies the, e signifies distance value and l denotes proportionality constant representing relationship among energy consumption as well as distance. Initially, the energy efficacy and communication range of SN in a WSN is assessed. The energy required by a transmitter to transfer a l -bit message in a distance e is expressed in equations (3) & (4).

$$F_{tr}(l, e) = \{l * F_{elec} + l * F_{gt} * e^2\} < e0 \quad (3)$$

$$e0 = \sqrt{\frac{F_{gt}}{F_{amp}}} \quad (4)$$

Where, $F_{tr}(l, e)$ indicates energy consumption of radio dissipation, F_{elec} signifies electronics energy based upon factors like digital coding, modulation, filtering, spreading of signal, $e0$ indicates first level energy, F_{gt} indicates free space, l signifies energy consumption of amplifying radio and F_{amp} represents the multiple path fading channel techniques based on the transmission distance e .

3.2 Spatial Bayesian Neural Network-based Network Construction

The network is constructed with Spatial Bayesian Neural Network (SBNN) [23] based hexagonal architecture, which improves network administration efficiency. The network contains four distinct types of hexagonal subdivisions, each with one parent node and four child nodes. The center point of the hexagon is found using the lattice point. By altering the model's complexity in response to the amount of data provided, the SBNN approach achieves model selection and prevents overfitting and under fitting issues. SBNN enable effective

transfer learning by incorporating prior knowledge into the model via the specification of prior distributions, which is especially useful when working with sparsely labeled data. The vectors t and φ represent the two dimensional Cartesian coordinate system used to define the lattice point expressed in equation (5).

$$\mathcal{G}_l(t; \varphi) = \exp \left[- \left(\frac{\|t - \psi_l\|}{\varphi} \right)^2 \right], \quad l = 1, \dots, L \quad (5)$$

Where, $\mathcal{G}_l$ represents the hexagon center point, ψ_l indicates the linear grouping of $\mathcal{G}_l$, t and φ represent the 2D Cartesian coordinate system. The hexagonal lattice vector model connects hexagonal lattice points using vectors. In this case, each hexagonal cell is represented by two vectors (t and φ). $\rho(\cdot)$ implies set of lattice points separated to hexagonal grids with L resolutions expressed in equation (6).

$$\rho(\cdot) = \mathcal{G}_1(\cdot)\beta_1 + \dots + \mathcal{G}_L(\cdot)\beta_L \quad (6)$$

Where, $\rho(\cdot)$ indicates lattice points, L represent the partition direction, $\mathcal{G}_l$ signifies whole lattices in vector space of 1st level, β_1 denotes objective function value, β_L indicates the Bayesian encoding. Each hexagon cell in σ has string of m numbers from x using equation (7).

$$\sigma_{m,jt}^x(t) = \text{softplus} \left(\left(\alpha_{m,j}^x \right) \mathcal{G}(t) \right) \quad (7)$$

Where, $\sigma_{m,jt}^x$ denotes grid part exceeding bottom m, jt and right corner at x , σ represents the hexagon cell, m signifies the number of cells, *softplus* indicates the logistic function, x signifies the threshold range, and $\mathcal{G}(t)$ signifies the sensor nodes. The grid in bottom right corner aligns with empty area in top left corner. The portions of the grid beyond the leftmost bottom and upper corners might coincide with the corresponding empty spaces. The SN are executed in the hexagon's center. This type of SBNN structure minimizes complexity in

network management. After network construction the results of this phase are fed into sensor authentication phase.

3.3 Authentication of sensors using Forward Private Verifiable Dynamic Searchable Symmetric Encryption

This section discusses Sensor Authentication with FPVDSSE [24]. The Secure Agent (SA) authenticates the SN based on their ID and location. The Secure Agent (SA) authenticates SN depending upon ID and location. Following registration, SA issues an authorization ticket with an FPVDSSE to ensure maximum security and minimum processing time. FPVDSSE ensures that users' search queries are secure and cannot be traced back to the original data owner. The encryption and key expansion procedures are part of the FPVDSSE algorithm. Five rounds are used in the proposed FPVDSSE for encryption and decryption, yielding five distinct keys. The length of the key should be much greater to guarantee security. After the key generating process comes encryption. Logical operations such as left period, swapping, and substitution are involved in the confusion and diffusion processes. Then, each round key is subjected to bitwise XNOR. Once the cipher key has been replaced initially is expressed in equation (8).

$$Dict[x] = (w^x, mcnt^x, valcnt^x) \quad (8)$$

Where, $Dict[x]$ indicates the cipher key, $Dict$ indicates dictionary created for every keywords w^x signifies the key expansion procedure, $mcnt^x$ denotes final counter of encrypted document for keyword x , $valcnt^x$ indicates secret key in forward index of document id . Encryption starts after the key generation process. This result in diffusion including confusion function is expressed in eqn (9).

$$wu = G_3(x \parallel (mcnt^x - 1) \oplus G_3(x \parallel mcnt^x) \oplus G_3(id)) \quad (9)$$

Where, wu signifies the output of the diffusion function, G_3 indicates the round key, $\oplus$ indicates the exclusive, x signifies the encrypted inverted index, id indicates the identifier of

the file. XNOR output is given to t operation to generate key expansions $mcnt$. These phases are repetitive in each round. The final round outcomes are combined to create the ciphertext tu_1 , which is expressed in equation (10).

$$tu_1 = (l_{w-1}^y, l_w^y, mcnt^y) \quad (10)$$

Where, tu_1 signifies the final merged round result, l_{w-1}^y indicates encryption key through version $w-1$ for keyword y , the function changes state of l by replacing $w-1$ with w , l_w^y signifies encryption key with version w for keyword y , $mcnt^y$ indicates the final counter of encrypted document of keyword y . Authentication and security were provided by a widely used data storage system. Finally, to improve security, data is encrypted and securely routed to authenticated sensor nodes. The blockchain stores authentication transactions, including both private and public blockchains. Following authentication, the clustering procedure begins to reduce energy consumption as well as latency.

3.4 Energy Efficient Clustering using Humboldt Squid Optimization Algorithm for Cluster Head selection

In this section, Humboldt Squid Optimization Algorithm (HSOA) is proposed [25] for Cluster Head selection, a bio-inspired optimization algorithm that achieves more rapid outcomes due to its high convergence. A minimum of two and a maximum of four nearest clusters are taken into consideration for simplicity and better outcomes and it is impacted if more clusters are combined and use more power for nodes. Clustering is performed by deploying a clustering agent on the edge server. Then clusters are given to cluster head selection. HSOA to obtain an optimal Cluster Head selection depend upon the parameters like Trust (T), Energy (E), Distance (Dist), Delay (D), Direction and Node Connectivity. The following is a model of the mathematically determined parameters used in cluster head selection and the parameters are given below.

Energy (E): For Cluster Head (CH) selection in Wireless Multimedia Sensor Network, energy denotes the power capacity that each node in the network has available to it. The selection of nodes as cluster heads and the formation of clusters are largely dependent on energy concerns using equation (11).

$$E^{energy} = \frac{E^{energy}(P)}{E^{energy}(S)} \quad (11)$$

Where, $E^{energy}(P)$ denotes the energy that exists between the CH and the network's base station (BS) and between the CH and the normal node and $E^{energy}(S)$ indicates energy of cluster head and energy of normal node.

Distance (D): Certain distance metrics are used by nodes to define their neighborhood in various clustering techniques. Which nodes are eligible to become cluster chiefs or members of a cluster can depend on this neighborhood distance using equation (12).

$$E^{Dist} = \frac{E^{Dist}(P)}{E^{Dist}(S)} \quad (12)$$

Where, $E^{Dist}(P)$ denotes distance among CH and network's base station (BS) and between CH and normal node and $E^{Dist}(S)$ specifies the distance among two normal nodes.

Delay (D): Nodes are required to transmit data with a predetermined delay, with a value that falls between 0 and 1. As a cluster's node count decreases, so does the delay, which is significantly reduced. In IoT, the total node count indicates the denominator value, and CH indicates the numerator value using equation (13).

$$E^{Delay} = \frac{\sum_{j=1}^m Max(CH)}{K} \quad (13)$$

Where, E^{Delay} indicates the overall delay between the CH and the normal node; $Max_{j=1}^m(CH)$

denotes the maximum transmission propagation in network's base station (BS); CH represents the cluster head selection and K indicates the size of packet.

Trust (T): Trust in cluster head selection refers to a network node's trust or conviction in choosing a specific node as cluster head in a cluster-based routing protocol. Trust is critical in determining the efficiency and dependability of the cluster head selection process in a multi-hop network as given in equation (14).

$$Trust = (credibility + reliability + intimacy) \div Self\ interest \quad (14)$$

Direction: Direction can be defined as the criteria or measure used to identify which sensor node should be chosen as the parameter for cluster head selection. This measure can be dependent on a range of parameters, including as the sensor node's proximity to other nodes and its communication capabilities. It is given in equation (15).

$$Direction = weight\ 1 * criterion\ 1 + weight\ 2 * criterion\ 2 + ... + weight\ n * criterion\ n \quad (15)$$

Where, $weight\ 1, 2 \& n$ represents the nodes weight, and $Criterion\ 1, 2 \& n$ represents CH value.

Node Connectivity: This parameter may be used to choose cluster heads in a network by considering nodes with better connection as prospective candidates. Nodes with higher connectedness are more likely to have stronger communication ties with other nodes in the network, making them ideal candidates for coordinating and controlling communication within a cluster as given in equation (16).

$$NodeConnectivity = (NDCN) / (TNNN) \quad (16)$$

Where, $NDCN$ signifies number of direct connections in node, $TNNN$ represents total amount of nodes in the network.

Cluster Head Selection:

HSOA is intended to efficiently explore huge solution spaces by replicating Humboldt squids' swarming behavior, allowing it to swiftly converge on near-optimal solutions. Humboldt squid hunting, mobility, and mating habits are the inspiration for HSOA. Attacking fish schools, running away, making successful attacks, larger squids attacking smaller ones, and mating are all part of the HSOA search process. Humboldt squid mate internally and lay millions of eggs. Females have a short lifespan and can lay up to 20 million eggs. This animal's movement, hunting, and mating behaviors are similar to optimizing a problem. Here, step by step process is defined for Cluster Head selection. The steps involved in the linearization technique it proposed using with the HSOA.

Step 1:Initialization

The position of each squid set in the search space at random is initialized. These positions show possible ways to address the optimization issue. It is given in equation (17).

$$Y_{new,j}^c = Y_a + S_{jet.}(-YM_{new,r_1}^c - popAll_{r_2}^c) \quad (17)$$

Where $Y_{new,j}^c$ represents the new position, Y_a represents the dimension, $S_{jet.}$ represents locomotion velocity parameter, YM_{new,r_1}^c represents new dimension position, r_1 random number among 1 as well as population size of fish, r_2 represents the random integer number amongst 2, $popAll_{r_2}^c$ represents size of fish population.

Step 2:Random generation

The cluster head selection randomly using aid of BOA algorithm approaches after initialization.

Step 3:Fitness function

Initialized evaluations utilized to generate random solution. It evaluated to select the optimal cluster head selection using equation (18),

$$Fitness Function = [cluster head selection] \quad (18)$$

Step 4: Successful attack

The coordinated efforts of the squid group to catch prey are usually necessary for a Humboldt squid attack to be successful. Before eating, the squids use their tentacles and sharp beaks to quickly bind and overpower their prey, mostly fish and crustaceans and it is given in equation (19),

$$YV_j^c = \begin{cases} YV_j = YV_{new,j} & \text{if } M_{V,newj} < M_{V,j} \\ successfulescape, & \text{otherwise} \end{cases} \quad (19)$$

Where YV_j^c represents the fitness of the Humboldt squids, YV_j represents the behaviour of Humboldt squid, $YV_{new,j}$ represents the new behaviour of Humboldt squid, $M_{V,newj}$ represents the domain of the squid, $M_{V,j}$ represents the hunting fish.

Step 5: Attack of stronger squids to smallest squids

If the fish and Humboldt squid do not find a better position in the preceding steps, it is assumed that there are no more fish to hunt. As a result, the larger Humboldt squids eat the smaller ones. In this stage, the Humboldt squid's position is derived from the equation (20).

$$YV_{new,j}^c = YV_{new,j}^c + S_{jet2}.(YV_{new,j}^c - Y_a^c) \quad (20)$$

Where $YV_{new,j}^c$ represents the new position of the fish, S_{jet2} represents the second velocity parameter, Y_a^c represents the better position of the squid.

Step 6: Humboldt squid mating

During their nightly hunts, Humboldt squid engage in complex courtship rituals that lead to mating. Males engage in intense rivalry, inserting sperm into the female's mantle chamber with the use of specialized tentacles. Before fertilization, females store sperm for several weeks. Afterwards, in deep waters, it laid thousands of eggs in gelatinous masses connected to substrates. It is given in equation (21).

$$G = CH\{\chi.\eta, (1-\eta).\chi, 1-\eta\} \quad (21)$$

Where G represents the egg position, CH indicates the cluster head selection, χ represents the squid eggs mass, η represents the adaptive weights.

Step 7: Termination

In this step, HSOA completes, best solution obtained through each process iterations returned as output, will repeat step 3 iteratively until halting criteria $Y = Y + 1$ is satisfied. The HSOA, processes are completed to cluster head selection where it attains optimal cluster head selection from the nodes.

3.5 Duty Cycling using Twin Actor Twin Delayed Deep Deterministic policy gradient

This step discusses Duty Cycling using TATD3 [26] is discussed. TATD3 increases sample efficiency by employing twin critics to estimate the Q-value. This dual-critic strategy lowers overestimation bias, resulting in more consistent and accurate Q-value estimates, which increases sample efficiency. TATD3 is capable of handling high-dimensional action spaces, making it appropriate for applications such as robotic control and continuous control problems in which the action space is continuous and higher dimensional. Sensor nodes continuously transmit data, resulting in high energy consumption. The scheduling agent, executed on the edge server, manages duty cycling. The system allocates time slots to every sensor and decreases data collisions during transmission using [27-28] TATD3-based duty cycling, which helps to save energy. It makes use of to lessen a single critic network's prediction inaccuracy. Higher precision and quicker convergence result from this. There are three modes in the proposed duty cycling process: idle, off, and on. All sensor nodes can send sensed data when they are in the ON mode. To prolong the life of TATD3, sensor nodes are switched off in OFF mode. Sensor nodes cannot transmit felt data when in IDLE mode; they can only receive it. Policy gradient-based TATD3 methods use to improve decoupling and minimize errors. The relationship and execution of the TATD3 is given in equation (22).

$$s(u) = \left(d_1^j h(g(f(u))) + d_1^j h \left(\sum_{u=0}^{(l-1)} g(f(u)) \right) \right) \quad (22)$$

Where, $s(u)$ indicates the actor TATD3 performs action, d_1^j signifies the policy function, h signifies the time slot, and $f(u)$ indicates exploration noise. The actor-network takes action $g(\cdot)$ depending on the current state and cycles through environment to observe the next state $l-1$ with a reward value of $d_1^j h$. The experience replay buffer will store information about $d_1^j h$. As a result, the actor's target network selects the correct next action $d_1^{jj} h$ depending upon the next state d_1^{jj} . At last, randomly selected sample data from the experience replay buffer are run by TATD3. It is expressed as equation (23).

$$s(u) = \left(d_1^{jj} h \left(g(f(u)) + d_1^{jj} h \left(\sum_{u=0}^{(l-1)} g(f(u)) + d_1^{jj} h(d_1^{jj} + g(\Delta f(u))) \right) \right) \right) \quad (23)$$

Where, $s(u)$ signifies the experience replay buffer information, $d_1^{jj} h$ indicates the sample data, d_1^{jj} signifies the computing value, u indicates the parameters of TATD3, $\Delta f(u)$ indicates the action of TATD3. The small value is regarded as ultimate target $\tilde{b}$ value. To reduce overestimating bias produced by continuous gathering and circulation. Adjust the duty cycling parameters as necessary to maximize power savings while maintaining functionality. It is expressed as equation (24).

$$UW = s + \phi \min_{\gamma D_{k>U}} (t', \tilde{b}), k \in \{1, 2\} \quad (24)$$

Where, U indicates the quality value, $\tilde{b}$ signifies the ultimate target, W signifies the value of discrimination, t' signifies the updated parameter value, s indicates the actor network state, $\min_{\gamma D_{k>U}}$ represents the lowest iteration episode, ϕ signifies the current completion time. Continuously parameter modifying and learning improves TATD3 training efficacy, resulting in optimal scheduling policies.

3.6 Secure multipath routing using Triple-Memristor Hopfield Neural Network

In this section, secure multipath routing using Triple-Memristor Hopfield Neural Network (TMHNN) 27 is discussed. TMHNN adds an additional degree of security to multipath routing. The network's capacity for remembering and storing patterns can be used to identify and prevent attacks or forbidden access to routing pathways. The neural network can constantly learn and adapt to changing network circumstances, making it ideal for dynamic applications. It may modify routing pathways in response to real-time events. Sensitive data is securely sent from source to destination. Before routing, data was divided into emergency and non-emergency categories based on size, deadline, and data type. The sensitive data is calculated as given in equation (25).

$$\gamma = \begin{cases} j = Y(\beta)v = b\beta v \\ d\beta / dt = ev - dh(\beta) \end{cases} \quad (25)$$

Where, γ represents the sensitive data multiple, e represents multiple generator, β represents the training instances, b represents the loss function, dh represents the constant variable, v represents the generators, Y indicates the discriminator, k represents routing agent, and dt represents the data size. The edge server has a routing agent installed in order to manage routing. The subsequent hop is determined by routing depending upon factors like energy, distance, trust, link quality. The link quality is expressed in eqn (26).

$$h_1(\beta) = \begin{cases} \beta - \sum_{j=1}^M (\tan h(r(\beta + (2j-1))) + \tan h(r(\beta - (2j-1))))_{\infty} \\ M = 1, 2, 3, \dots \end{cases} \quad (26)$$

Where, $h_1(\beta)$ represents the link quality value, r represents the majority of real adversarial model attacks, M denotes the training apprentice value, and h indicates the maximum allowable disparity between the original data. The optimal route is chosen depending upon factors like packet delivery ratio, hop count, and network reliability. The leader makes a

choice, and other players or followers to determine own activities. The discriminator serves as the leader as given in equation (27).

$$d\beta / dt = -dh(\beta) \quad (27)$$

Where, $d\beta/dt$ represents the discriminator server, and $-dh$ represents the negative multiple generator. Training is adjusted between discriminator and generator. The discriminator's output is generator successfully misleads the discriminator. Each generator and discriminator pair is assigned an equal weight. The weight of generator is expressed in equation (28).

$$E_j \dot{y}_j = -\frac{z_j}{S_j} + \sum_{k=1}^m y_{jk} \tanh(z_k) + J_j \quad (j, k \in M^*) \quad (28)$$

Where, E_j represents the weight of generator, z represents the probability of the j^{th} class, J_j represents the minimum value, and S_j represents the path selection matrix. The impacts of gradient-based untargeted attacks are greatly mitigated by this strategy. TMHNN selects the best path among various alternatives. The system prioritized routing paths depending on the number of hops from source to destination. Backup agents then choose an alternate route and install it on the blockchain. TMHNN minimizes node and routing failures owing to energy depletion and incorrect data. Finally, multipath routing is done by using TMHNN. In this work, for WSN based secure-multipath routing, this method optimizes the TMHNN optimum parameter E_j and β utilizing LEOA employed to enhance the TMHNN. The LEOA used to adjust the TMHNN weight parameter.

3.7 Optimization using Lotus Effect Optimization Algorithm

The weights parameter E_j and β of TMHNN is enhanced with the Lotus Effect Optimization Algorithm (LEOA) [28]. The weight parameter E_j is optimized to increasing the Network Lifetime and β is optimized to decreasing the energy consumption. The lotus leaf's super-hydrophobic and self-cleaning properties are indicated by its effect. Water collects on the

plant's leaves and slides down them without being absorbed due to a characteristic of the leaves. The two primary processes involved in pollination are the biological (cross-pollination) as well as non-biological processes (self-pollination) that represented by LEOA's exploration and removal stages.

3.7.1 Stepwise process of LEOA

The sequential process is clear to attain optimal values of TMHNN utilizing LEOA. Initially, LEOA makes the uniformly distributed population for enhancing optimal parameters of TMHNN parameters.

Step 1: Initialization

The population in LEOA has to be initialized by generating a collection of random solutions. It can use the following matrix to indicate that each Lotus Effect Optimization Procedure is given equation (29).

$$D = \begin{bmatrix} D_1^1 & D_1^2 & \dots & \dots & D_1^b \\ D_2^1 & D_2^2 & \dots & \dots & D_2^b \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ D_n^1 & D_n^2 & \dots & \dots & D_n^b \end{bmatrix} \quad (29)$$

Where, the goal is to minimize to function, the step mass should be chosen so that it minimizes the function worth at the new idea and n is the number of paths, b is the execution paths. The best solution is promoted utilizing LEOA method then equivalent flowchart is certain in Figure 2.

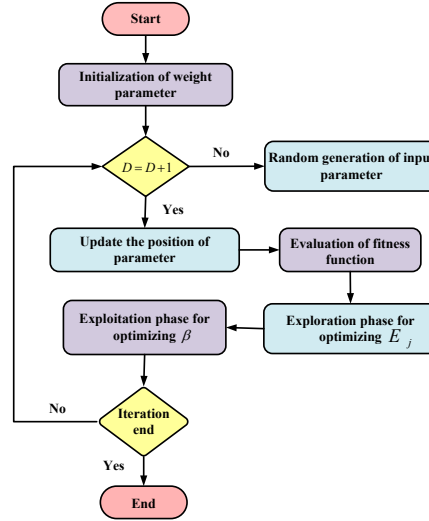


Figure 2: LEOA for enhancing TMHNN parameter

Step 2: Random generation

Input parameters are created randomly after initialization. Ideal fitness values are chosen depend on clear hyper parameter condition.

Step 3: Fitness function

Random solution creates initialized assessments. Fitness function is evaluated for optimizing weight parameter E_j and β of the WSN based secure-multipath routing using parameter optimization value. It is computed by eqn (30).

$$\text{Fitness Function} = \text{optimizing } [E_j \text{ and } \beta] \quad (30)$$

Where, E_j is optimized to increasing the Network Lifetime and β is optimized to decreasing the energy consumption.

Step 4: Exploration phase for optimizing E_j

Dragonflies carry out global pollination that is the same as the suggested algorithm's exploratory phase in the LEOA. The dragonfly algorithm takes into account two ideas of food and enemy in addition to three fundamental characteristics of insect swarms: separation, alignment, and cohesiveness. Then, calculates the evaluation of each optimization vector is given in the equation (31).

$$T_a^s = \sum_{b=1}^Z Y_a^s - E_j Y_b^s \quad (31)$$

Where T_a^s denotes the current position, $\sum_{b=1}^Z$ represents the amount of entities in the neighborhood, Y_a^s is the current being's spot with directory in completion repetition, E_j is used to increasing the Network Lifetime, and Y_b^s is position of separate neighborhood in growth iteration.

Step 5: Exploitation phase for optimizing β

The exploitation phase is local pollination, or self-fertilization. A coefficient specifies the scope of every blossom's growing area around the finest-discovered flower in this kind of auto gamy. At the beginning of the motion procedure, the phases are engaged more slowly, and at the end, it is engaged quicker. It is given in equation (32).

$$Y_a^{s+1} = Y_a^s + Q(\beta - e^*) \quad (32)$$

Where, Y_a^{s+1} denotes the current number of iterations, Y indicates the growth area, Q is the exploitation movement, e^* signifies the found pollen position among all growth iterations, β is used to decreasing the energy consumption.

Step 6: Termination Condition

With the aid of LEOA, the weight parameter value E_j and β from the TMHNN are optimized using LEOA, repeat step 3 iteratively till fulfil halting criteria $D = D + 1$. Then, SMR-OTMHNN-WSN method effectively identify the terms with high Network Lifetime and low energy consumption.

4. Result with Discussion

In this part, performance analysis of the proposed SMR-OTMHNN-WSN is illustrated and it is implemented in Python and server running Windows 7 with a 64-bit 2.9GHz CPU and 4 GB of primary RAM. The performance of the proposed method is examined using mentioned

metric. The SMR-OTMHNN-WS technique is compared with existing SEE-DL-WSN 16, PSO-GWO-SEE-WSN 17, and EE-WSN-MC-DL 18 techniques.

Parameters	Value	Parameters	Value
No. of edge servers	10	No. of sensor nodes	120
Packet count	200	Transmission range	200 m
Number of slots	15	Slot Length	1050 bits
Secure Agent	1	Slot Duration	9 μ s
Initial energy	100 J	Modules	Wi-Fi, internet, IPV4
Packet data rate	100 Mbps	Blockchain	1
Cloud server	1	Packet interval	0.5 s
Traffic type	UDP, TCP/IP	Node mobility	10 m/s
Simulation area	900 $\times$ 1200 m^2	Size of Packet	64, 128,...,1024 bytes

4.1 Performance metrics

The efficiency of the proposed method is examined under several performances metrics such as Energy consumption, Latency, Throughput, Packet Delivery Ratio, Network Lifetime, and Alive nodes. The following metrics are required to scale the performance metrics.

4.1.1 Energy consumption

The metric signifies energy expended with node in network. It is calculated using equation (33).

$$EnergyConsumption = \left[\sum_{N=1} CH_x(u) + \sum_{A=1} CM_x(a) \right] \quad (33)$$

Where, energy utilized by CH is designated as $CH_x(u)$ then energy utilized by cluster member defined as $CM_x(a)$.

4.1.2 Latency

The time consumed for a request to travel from sender to receiver and back again. The formula for latency is in equation (34).

$$Latency = RTT/2 \quad (34)$$

Where, RTT indicates Round Trip Time taken for a request to move from sender to receiver.

4.1.3 Throughput

It measures the proportion of successful retrievals in a given simulation time. If the performance value is higher, then the network is considered more secure and efficient is given in equation (35).

$$Throughput = \frac{\sum \text{Successfully received data packets at destination}}{\text{Simulation time} * 1024} \quad (35)$$

4.1.4 Packet delivery ratio

The number of data packets distributed efficiently in base station through altered number of nodes. This is calculated using equation (36).

$$Packet\ delivery\ ratio = \frac{\sum \text{No. of packets received}}{\sum \text{no. of packets sent}} \times 100\% \quad (36)$$

4.1.5 Network lifetime

It identifies how long or how many rounds network conduct activities. It is the time interval during which all nodes in the network collapse. This is calculated by equation (37).

$$Network\ lifetime = \min_x \left[\frac{\sum_{x=1} AL_{td} * K_t}{N_x} \right] \quad (37)$$

Where, AL_{td} denotes coverage matrix, K_t denotes life of node, N_x denotes number of nodes attention.

4.1.6 Alive nodes

This parameter represents nodes within networks that have enough energy to complete their duties and it is given by the equation (38),

$$K_I^f = W_{Rec}^f(r) > 0 \quad (38)$$

Here, K_I^f denotes number of alive nodes, $W_{Rec}^f(r)$ represents the remaining energy node in f^{th} round.

4.2 Performance Analysis

Figure 3-8 determines simulation outcomes of SMR-OTMHNN-WSN technique. Then, the proposed SMR-OTMHNN-WSN method when compared with existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL models.

Figure 3 shows energy consumption analysis. The LotusEffect Optimization method is renowned for its ability to identify optimal solutions to complicated situations. This makes it especially useful for multi-path routing, where several pathways must be identified and optimized. Here, the proposed SMR-OTMHNN-WSN attains 14.25%, 21.25%, and 18.27% lower energy consumption at 70 rounds; and 17.98%, and 24.46% and 12.01% lower energy consumption at 100 rounds when compared to the existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods.

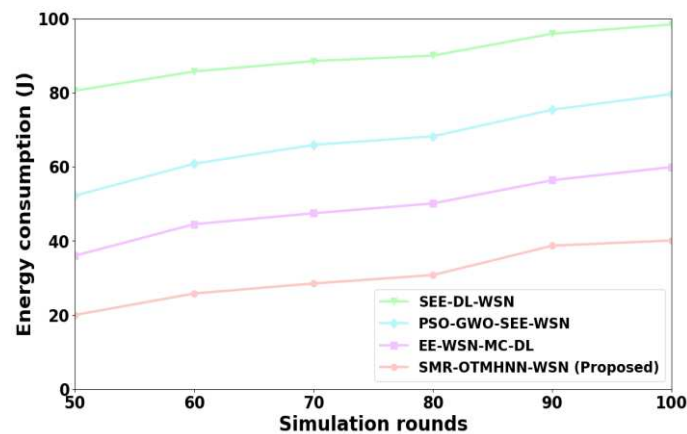


Figure 3:Energy Consumption analysis

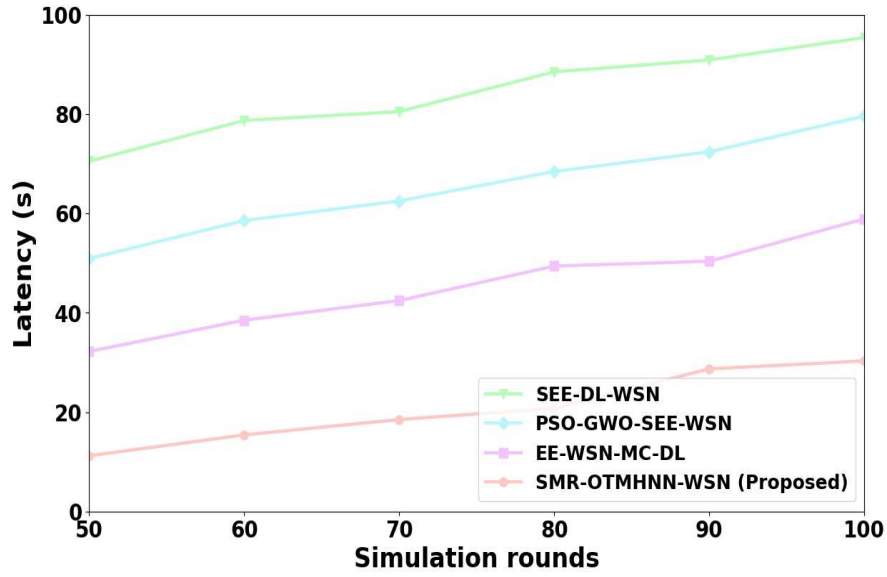


Figure 4:Latency analysis

Figure 4 shows Latency analysis. The graph shows the latency metrics for each path in the multipath routing configuration. Each path might impose a data series on the graph. Here, the proposed SMR-OTMHNN-WSN attains 15.25%, 23.25%, and 17.27% lower Latency at 80 rounds; and 16.98%, and 23.46% and 11.01% lower Latency at 100 rounds when compared to the existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods.

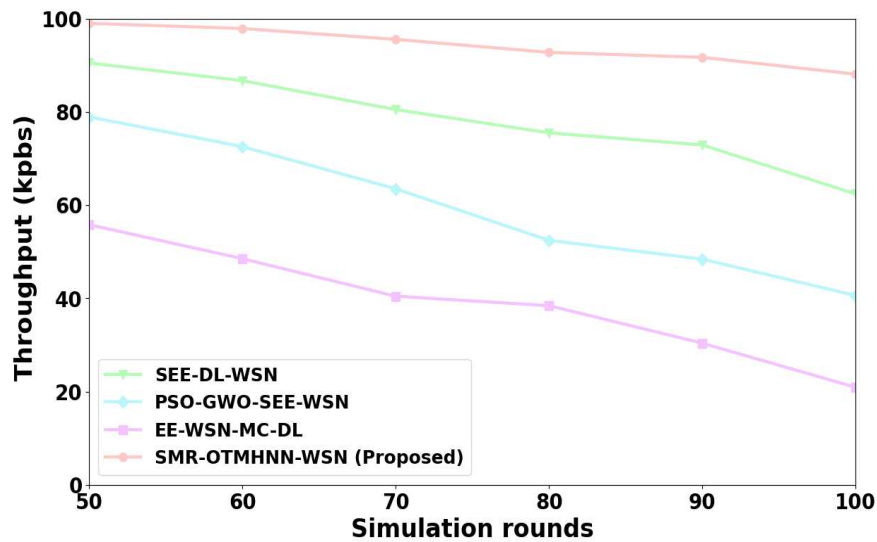


Figure 5: Throughput analysis

Figure 5 shows Throughput analysis. LEO is a reasonably straightforward algorithm to implement, b making it accessible to academics and practitioners across a wide range of areas. Here, the proposed SMR-OTMHNN-WSN attains 19.59%, 24.69% and 16.89% higher Throughput at 60 rounds; and 16.58%, 22.26% and 21.78% higher Throughput at 100 rounds evaluated with existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods.

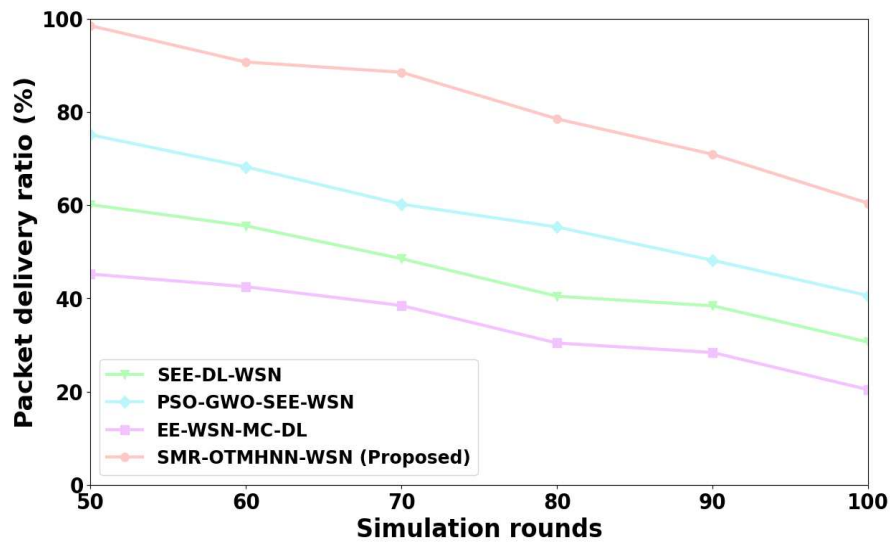


Figure 6: Packet Delivery Ratioanalysis

Figure 6 depicts packet delivery ratio analysis. The technique can readily scale to handle a large number of pathways, making it appropriate for high-complexity applications. These advantages of the TMHNN help the proposed method to attain higher Packet Delivery Ratio. Here, the proposed SMR-OTMHNN-WSNattains18.79%, 25.41% and 26.94% higher Packet Delivery Ratio at 70 rounds; and 16.58%, 23.29% and 27.98% higher Packet Delivery Ratio at 100 roundswhen compared to the existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL techniques.

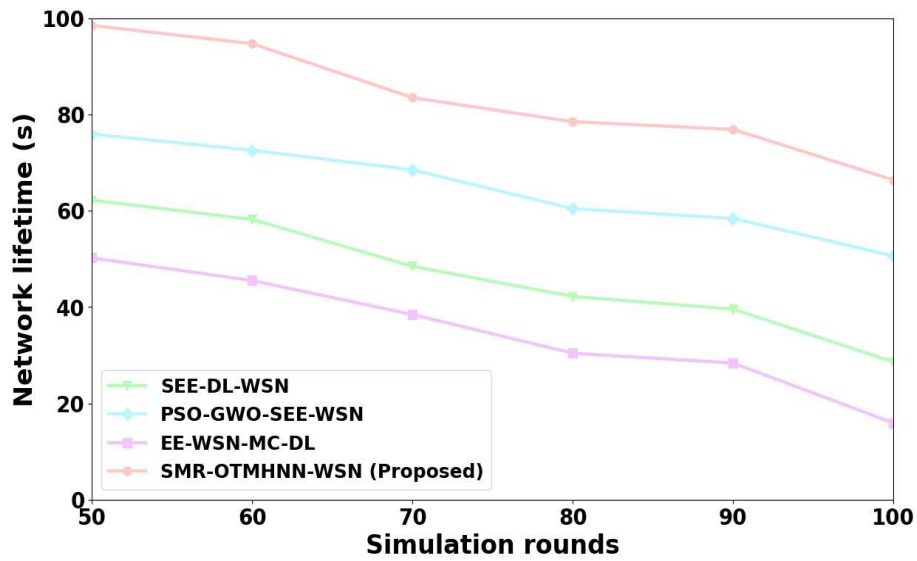


Figure 7: Network Lifetime analysis

Figure 7 depicts network lifetime analysis. The graph typically depicts the network nodes' remaining energy over time, with the x-axis indicating time and the y-axis illustrating energy levels. Here, the proposed SMR-OTMHNN-WSN attains 19.79%, 27.41% and 24.94% higher Network Lifetime at 60 rounds; 17.35%, 23.58% , 27.29% greater Network Lifetime at 80 rounds; 19.58%, 25.29% , 29.98% greater Network Lifetime at 100 rounds when compared to the existing as SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL respectively.

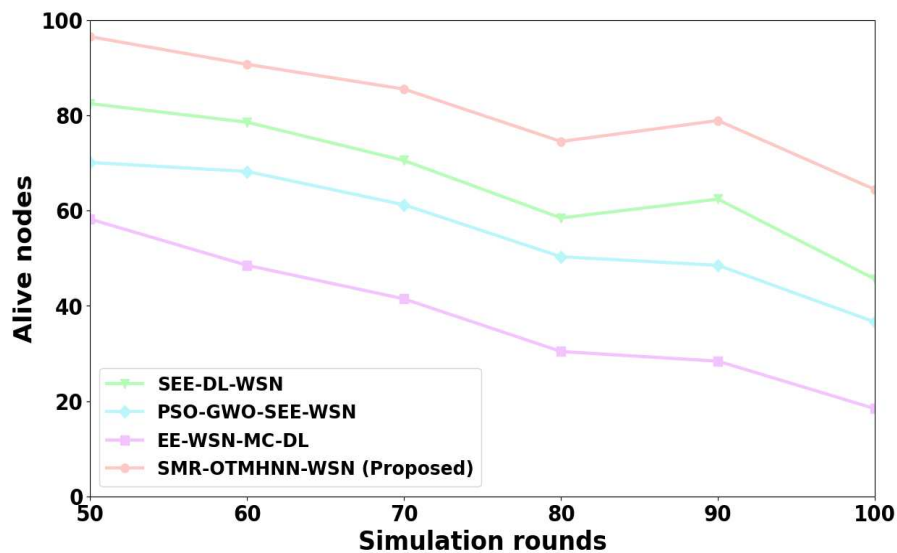


Figure 8: Performance Analysis of Alive nodes

Figure 8 depicts alive nodes analysis. This graph depicts the overall health and connectivity of the network. Proposed SMR-OTMHNN-WSN technique then provides 17.95%, 22.95% and 26.47% higher alive nodes at sum of rounds 60; 16.80%, 19.40% and 22.64% greater count of alive nodes at count of rounds 80; 23.67%, 20.98% and 31.34% greater number of alive nodes in number of rounds 100; evaluated to existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods.

4.3 Discussion

In this work, SMR-OTMHNN-WSN model for Energy-Efficient Routing of IoT-Based WSN Environment is discussed. Dynamic clustering employing HSOA improves communication reliability while reducing energy usage during data collecting and aggregation. Clustering takes time due to slow convergence, resulting in high energy consumption and latency. HSOA optimizes the CH created on distance, energy, security, and delay, increasing complexity. Fuzzy logic is used to approximate values, reducing overall security. HSOA clustering method, which incorporates distance and energy, is insufficient for optimum CH selection. Static CH selection causes energy depletion and increased data loss. This research uses the TMHNN algorithm to execute safe routing and minimize network congestion, resulting in quicker and less delayed data transfer. The proposed paradigm addresses the shortcomings of HSOA, which provides safe routing based on node trust values but lacks data security. The HSOA algorithm used to find intercluster data transmission paths. The lack of discrete time periods for sensors leads to increased latency. The proposed SMR-OTMHNN-WSN method is examined using several performance metrics. Here, presenting a comparison of the 99.43 J Energy Consumption; 94.64 s Network Lifetime; 93.96 kbps throughput; and 94.23% packet delivery ratio; achieved by the proposed technique to that of SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods.

5. Conclusion

In this manuscript, SMR-OTMHNN-WSN is successfully implemented. Initially, every SN is reused in a SBNN-based structure to improve network management and reduce complexity from random deployment. The system uses FPVDSSE to authenticate all sensor nodes, ensuring high security against external attacks. The HSOA is utilized for dynamic CH selection and clustering based on time and event parameters in order to increase energy economy and decrease latency. By doing this, the environment's throughput is increased and good communication validity is guaranteed. The TATD3 algorithm extends the lifetime of the network by reducing energy consumption through duty cycling that is adjusted to the present environment. Subsequently, the system employs multipath and secure routing (TMHNN) to guarantee secure and efficient data transfer. Before data is transmitted, FPVDSSE encrypts it to increase throughput and lower packet loss from mistakes. Throughput is enhanced as the backup agent chooses other routes to minimize data loss arising from sensor nodes' lack of energy. The performance of the proposed SMR-OTMHNN-WSN approach contains 19.59%, 24.69% and 16.89% higher Throughput; 15.25%, 23.25%, and 17.27% lower Latency; and 17.95%, 22.95% and 26.47% higher alive nodes; are compared with existing SEE-DL-WSN, PSO-GWO-SEE-WSN, and EE-WSN-MC-DL methods. In future, this proposed method aims to connect software defined network (SDN) using IoT to improve network administration, scalability, and flexibility.

Ethical Approval and Consent to participate: This article does not contain any studies with human participants performed by any of the authors.

Human and Animal Ethics: Not Applicable

Consent for publication: Not Applicable

Availability of supporting data: The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Materials and Methods: Not applicable

Results and Discussions: Not applicable

Declarations: Not applicable

Conflicts of interest/Competing interests: Not applicable

Acknowledgements: Not applicable

Authors' contributions

Dr. Kamalakkannan D. (Corresponding Author): *Conceptualization, Methodology, Original draft preparation*

Mrs. Parul Awasthi: *Supervision*

Mr. Shaman Bhat: *Supervision*

Mrs. Monali Shetty: *Supervision*

Reference

- [1] Khan ZA, Amjad S, Ahmed F, Almasoud AM, Imran M, Javaid N. A blockchain-based deep-learning-driven architecture for quality routing in wireless sensor networks. *IEEE Access*. 2023;11:31036-51.
- [2] Jadav NK, Gupta R, Alshehri MD, Mankodiya H, Tanwar S, Kumar N. Deep learning and onion routing-based collaborative intelligence framework for smart homes underlying 6g networks. *IEEE Transactions on Network and Service Management*. 2022;19(3):3401-12.
- [3] Rajasoundaran S, Kumar SS, Selvi M, Ganapathy S, Rakesh R, Kannan A. Machine learning based volatile block chain construction for secure routing in decentralized military sensor networks. *Wireless Networks*. 2021;27(7):4513-34.

- [4] Kipongo J, Swart TG, Esenogho E. Artificial Intelligence-Based Intrusion Detection and Prevention in Edge-Assisted SDWSN With Modified Honeycomb Structure. IEEE access. 2023.
- [5] Alsamhi SH, Almalki FA, Afghah F, Hawbani A, Shvetsov AV, Lee B, Song H. Drones' edge intelligence over smart environments in B5G: Blockchain and federated learning synergy. IEEE Transactions on Green Communications and Networking. 2021;6(1):295-312.
- [6] Haseeb K, Din IU, Almogren A, Ahmed I, Guizani M. Intelligent and secure edge-enabled computing model for sustainable cities using green internet of things. Sustainable Cities and Society. 2021;68:102779.
- [7] Sharmila AH, Jaisankar N. Edge intelligent agent assisted hybrid hierarchical blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT. Computer Networks. 2021;200:108508.
- [8] Nouman M, Qasim U, Nasir H, Almasoud A, Imran M, Javaid N. Malicious node detection using machine learning and distributed data storage using blockchain in WSNs. IEEE Access. 2023;11:6106-21.
- [9] Haseeb K, Alruwaili FF, Khan A, Alam T, Wafa A, Khan AR. AI Assisted Energy Optimized Sustainable Model for Secured Routing in Mobile Wireless Sensor Network. Mobile Networks and Applications. 2024:1-9.
- [10] Saba T, Rehman A, Haseeb K, Bahaj SA, Lloret J. Trust-based decentralized blockchain system with machine learning using Internet of agriculture things. Computers and Electrical Engineering. 2023;108:108674.
- [11] Janarthanan A, Vidhusha V. Cycle-Consistent Generative Adversarial Network and Crypto Hash Signature Token-based Block chain Technology for Data Aggregation

- with Secured Routing in Wireless Sensor Networks. *International Journal of Communication Systems*. 2024;37(4):e5675.
- [12] Zhang D, Yu FR, Yang R. Blockchain-based multi-access edge computing for future vehicular networks: A deep compressed neural network approach. *IEEE Transactions on Intelligent Transportation Systems*. 2021;23(8):12161-75.
- [13] Ilakkiya N, Rajaram A. A secured trusted routing using the structure of a novel directed acyclic graph-blockchain in mobile ad hoc network internet of things environment. *Multimedia Tools and Applications*. 2024:1-26.
- [14] Abbas S, Javaid N, Almogren A, Gulfam SM, Ahmed A, Radwan A. Securing genetic algorithm enabled SDN routing for blockchain based Internet of Things. *IEEE Access*. 2021;9:139739-54.
- [15] Bhuvaneswari CA, Ruby EK. Block chain technology for secured dynamic optimal routing in WSN with optimized generative adversarial capsule network. *International Journal of Communication Systems*. 2024;37(6):e5711.
- [16] Prasad KV, Periyasamy S. Secure-Energy Efficient Bio-Inspired Clustering and Deep Learning based Routing using Blockchain for Edge Assisted WSN Environment. *IEEE Access*. 2023.
- [17] Prithi S, Sumathi S. Automata based hybrid PSO–GWO algorithm for secured energy efficient optimal routing in wireless sensor network. *Wireless personal communications*. 2021;117:545-59.
- [18] Montoya GA, Lozano-Garzón C, Donoso Y. Energy-Efficient and Delay Sensitive Routing Paths Using Mobility Prediction in Mobile WSN: Mathematical Optimization, Markov Chains, and Deep Learning Approaches. *IEEE Access*. 2021;9:153382-400.

- [19] Sharma A, Kansal A. Advanced ANN based secured energy efficient routing protocol in WSN. *Wireless Personal Communications*. 2023;132(4):2645-66.
- [20] Gurram GV, Shariff NC, Biradar RL. A secure energy aware meta-heuristic routing protocol (SEAMHR) for sustainable IoT-wireless sensor network (WSN). *Theoretical Computer Science*. 2022;930:63-76.
- [21] Dinesh K, Svn SK. GWO-SMSLO: Grey wolf optimization based clustering with secured modified Sea Lion optimization routing algorithm in wireless sensor networks. *Peer-to-Peer Networking and Applications*. 2024;17(2):585-611.
- [22] Gulganwa P, Jain S. EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. *International Journal of Information Technology*. 2022;14(1):135-44.
- [23] Zammit-Mangion A, Kaminski MD, Tran BH, Filippone M, Cressie N. Spatial Bayesian neural networks. *Spatial Statistics*. 2024:100825.
- [24] Guo C, Li W, Tang X, Choo KK, Liu Y. Forward private verifiable dynamic searchable symmetric encryption with efficient conjunctive query. *IEEE Transactions on Dependable and Secure Computing*. 2023;21(2):746-63.
- [25] Anaraki MV, Farzin S. Humboldt Squid Optimization Algorithm (HSOA): A novel nature-inspired technique for solving optimization problems. *IEEE Access*. 2023;11:122069-115.
- [26] Joshi T, Makker S, Kodamana H, Kandath H. Twin actor twin delayed deep deterministic policy gradient (TATD3) learning for batch process control. *Computers & Chemical Engineering*. 2021;155:107527.
- [27] Lin H, Wang C, Yu F, Hong Q, Xu C, Sun Y. A triple-memristor Hopfield neural network with space multistructure attractors and space initial-offset behaviors. *IEEE*

Transactions on Computer-Aided Design of Integrated Circuits and Systems.
2023;42(12):4948-58.

- [28] Dalirinia E, Jalali M, Yaghoobi M, Tabatabaee H. Lotus effect optimization algorithm (LEA): a lotus nature-inspired algorithm for engineering design optimization. The Journal of Supercomputing. 2024;80(1):761-99.