SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I2P108

Volume 12 Issue 2, 86-94, February 2025

Original Article

Bald Eagle Search Optimized Deep CNN-Based Routing Scheme for WSN Using IoT-Based Blockchain Technology

G. Sugitha[1], S. Maheswari[2], D. Karthikeyan[3], V. Asha[4]

[1]*Department of Computer Science and Engineering, Muthayammal Engineering College (Autonomous), Rasipuram, Namakal, Tamilnadu, India.*
[2]*Department of Computer Science and Engineering, Nandha Engineering College, Erode, Tamilnadu, India.*
[3]*Department of Electrical and Electronics Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, Tamil Nadu, India.*
[4]*Department of Computer Applications, New Horizon College of Engineering, Bengaluru, Karnataka, India.*

[1]*Corresponding Author : sugitha1091@gmail.com*

Received: 10 December 2024 Revised: 08 January 2025 Accepted: 09 February 2025 Published: 26 February 2025

Abstract *- Wireless Sensor Networks (WSN) with changing environments are potentially vulnerable to various forms of threatening cyber-attacks, and they rely heavily on encryption and authentication techniques to tackle this problem. Because of the present changes in routing data, most prevalent routing algorithms face failure in characterizing harmful network nodes. Regarding the cybersecurity challenges of Internet of Things (IoT) devices, it's a critical desire to identify novel approaches that improve the overall safety of WSNs. A problem that requires consideration is IoT device data storage and secure management. More existing determinations rely on a centralized framework, ecosystems are easy to interfere with, and data obtained from sensors are not authentic. Thus, this work presents a trustworthy and secure inter-correlated routing strategy that depends on the IoT-based blockchain, optimization algorithm, and deep learning techniques. The distributed routing data in the WSN is managed by the blockchain method, which achieves the best possible routing with the assistance of the Bald Eagle Search Optimization (BES) algorithm. The Deep Convolutional Neural Network (DCNN) algorithm makes effective routing decisions based on routing information variations among the nodes. The suggested routing strategy is carried out, and its efficacy is measured using latency, energy usage and throughput parameters. The suggested approach's performance is enhanced to high efficiency, and it is evaluated for malicious attacks and delays.*

Keywords *- WSN, IoT, BES algorithm, DCNN, Blockchain.*

1. Introduction

WSNs are wireless networks comprising multiple sensor nodes indicated for determining physical conditions in the surroundings [1-3]. WSNs are employed in various applications, including home automation, industrial, military, wellness, environmental protection, commerce and mobility [4, 5]. Each region can accommodate hundreds of applications. Communications among nodes are considered unreliable due to the reason of a secure wireless channel. To avoid such security breaches, authentication is essential. In WSN, data authentication enables the system to validate whether data has been delivered from an approved origin. It protects the authentic data from variations. Authentication is critical for WSN connection security [6]. While communication among the sensor nodes, authentication ensures that the origin node recognizes the node to which it delivered the data as an original node. Individual sensor nodes that have been authorized are permitted to link the network, and other nodes do not have the ability to do that. Unauthorized users are thereby prohibited from accessing the network in this manner [7-9].

IoT-based blockchain is an emerging technology that provides excellent secure outcomes in WSN. Solutions depending on blockchain and smart contracts are capable of performing network authentication and access control [10, 11]. Although the WSN sensor nodes are considered to have a restricted amount of space, it is necessary to link the blockchain and WSN organized without raising energy consumption and surplus transactions for the purpose of exploiting the significant characteristics of blockchain to suit the WSN's security needs [12, 13]. Threats in WSNs are typically recognized in two distinct manners: one through routing and the other through data. Routing attacks are carried out by selecting an improper path to the required protocol. The

malicious node will pick the most energetic route, for instance, if the routing protocol is selecting an energy-effective route [14-16]. This, in turn, shortens the lifecycle of the network, damages the energy of the majority of sensors, and raises the transmission frequency. Data threats occur when a malicious node plays with the encoded data in the package to make changes or to discover transmission data. The two factors that are having the biggest impact on WSN communication efficiency are data security and route security.

There are several established methods for enforcing reliable routing. Some methods take into consideration the sensor's power when determining which nodes throughout the path are reliable [17, 18]. The quantity of energy used for each transmission determines the potential remaining energy in the sensors. That allows for the measurement of node trustworthiness. Similar to this, some systems gather feedback from several intermediate nodes in order to determine the nodes' level of dependability [19, 20]. Nevertheless, this extends the network maintenance costs and impacts transmission performance. Similarly, numerous algorithms are accessible, but their efficacy is not sufficient. Henceforth, this paper proposes an optimal routing method named BES-optimized Deep CNN, which is used for the efficient transmission of data. Moreover, it offers high accuracy with minimized data losses for secured data transmission. The major contribution of this research is are the following:

- This paper uses blockchain technology to put forward a determination for secured data transmission obtained from IoT devices.
- A BES-optimized deep CNN routing system is presented, which assures energy-effective data transfer from one node to another.
- This BES-optimized deep CNN ensures secure and dependable data transmission.

2. Proposed System

This work implements an IoT-based blockchain technology to ensure the stability and dependability of WSN path information. As illustrated in Figure 1, the data traceability and tamper-proof into the WSN is able to store additional data related to each node utilizing blockchain token transactions.

The blockchain-based routing system is divided into two sections: a blockchain and a real routing network, which includes three types of organizations: server nodes, terminal devices and routing nodes. Each node links the terminals via its specific LAN and transfers packet data received from other routing nodes to particular destinations (targets). In the beginning, the information gathered from the IoT sensor is transmitted to the source terminal. R_1. This R_1 delivers a packet of data to the initial routing node R_2, and the network routing R_3 transmits these data to the next stage node R_D using a deep learning-based routing rule. This deep learning model requests and accumulates state data essential to the routing network in continuous time. Each blockchain has an accurate consensus method to ensure the equity of transactions. PoA consensus technique is preferred here to boost transaction efficiency. The server and routing nodes are represented by the PoA-based blockchain network, which is classified into two categories: validator and minion. At this point in the work of the blockchain network, each server node is referred to as a validator, which also holds one blockchain address. It entails some specialized activities, such as verifyingemitting blocks, transaction block chains and implementing smart contracts. The minion differs from the validator, which performs responsibilities such as token contract, information transfer validation, and contract function activation. Lastly, the decision of the shortest path selection is verified using BES-optimized DCNN, which is explained in depth in the following section.

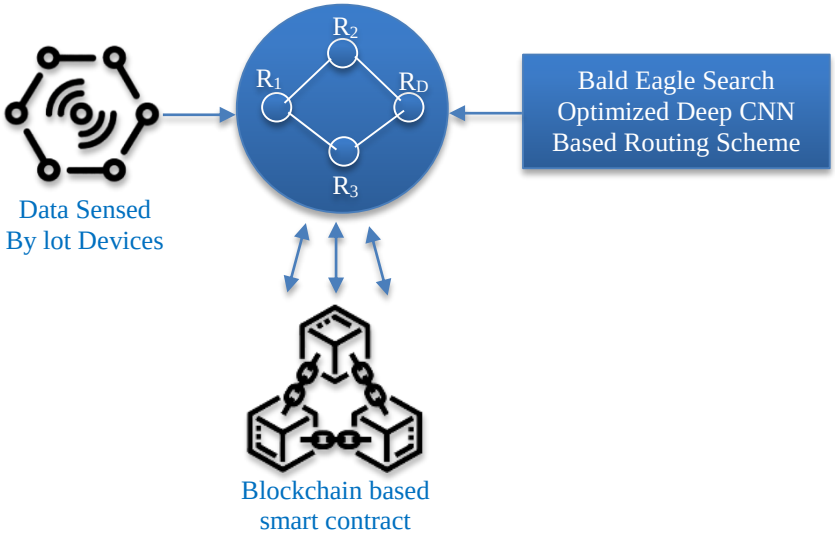

Fig. 1 IoT-based blockchain technology using optimized DCNN

2.1. Block Chain Network Procedure

The blockchain network design is applicable to efficiently operate by modifying and sending information about network routing stored in smart contracts. Following that, the data contained in the smart contracts, including token, blockchain, and registration, is checked utilizing an approved server node and upgraded in the blockchain network.

Algorithm 1. *Registration contract*

Input: BC_{add} *and* PHY_{add}

Output: *Registered node* R_n

1 *Map*: $BC_{add} = PHY_{add}$

2 *State*: $BC_{add} = Zero/one$

3 *While authentic means do*
/trigger the contract call functions/

4 $R_n = Zero$

5 *If state* $(BC) = One$: *then*

6 $Stop/R_n$ *is successfully registered*

7 *Else*

8 *map* $(BC_{add}) = PHY_{add}$

9 *State* $(BC_{add}) = one$

10 *The* R_n *is successfully registered*

11 *end if*

12 *End while*

By connecting the whole server nodes in the system, the physical address (PHY_{add}) of all routing nodes has been entered in the registration contract. Algorithm 1 explains the process to set up the contract's server nodes. The registration contract's localization phase gives knowledge about the nodes, including the probability that the nodes are currently registered. Whenever an additional network node must be registered, the structure is active, and the registration contract is transmitted. The registration contract first verifies to determine whether the blockchain location already exists in the statemap. If the state mapping is "one", then the blockchain address (BC_{add}) have been existing, indicating that the required node has been assigned. If the state mapping is "zero," registration of the node (R_n); $n = 1,2,\ldots$ is capable of being completed satisfactorily.

2.1.1. Block Chain Transaction Steps

In the routing node R_n, initially fix the no.of packets as h. Likewise, in the routing nodeR_1, the no.of packets is s, therefore $TBR_i = h$ *and* $TBR_j = s$. In the beginning, the m packets data to the next stage routing (R_2). While transferring the packets, the routing node R_n delivers the transfer data to the contract of the token. The transfer function provides data related to state changes, such as the amount of packets transported, the next node, etc. Following the arrival of$'m'$ unit packets, the token amount of discharge$'n'$ and the R_2 to the blockchain network via the message on the token contract.$'m'$ is the no. of packets obtained by the routing node R_2. The token contract checks whether$'m = m'$ after getting the confirm message. By authenticating the approved server for transferring the node conversion to the block chain network, the PoA consensus process successfully finishes these token transactional procedures. Unauthorized activities are disregarded and not published in the blockchain network, which results in no data loss.

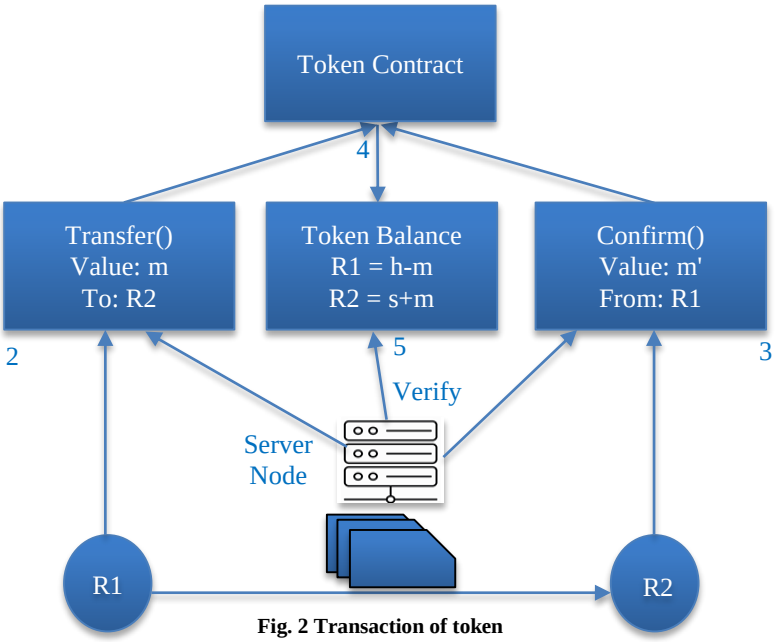

Fig. 2 Transaction of token

Each transaction recorder in Figure 2 is equipped with the timestamp, route address at each hop, token name, and number of tokens communicated. Furthermore, the backup for token transaction data for obtainable accountability is contained throughout the complete server node and routing node. Thus, in this network, R_n has a chance to acquire and compose a claim of routing data periodically based on the routing planning model. This network routing algorithm provides the current routing algorithm with a reliable basis for routing. Additionally, an improvement to the suggested model is required for the routing information to be used effectively. Therefore, the DCNN is used for monitoring any modifications in the routing data and for choosing the best routing options to enhance the implementation and flexible functioning of the block chain routing planning model.

2.1.2. Deep Convolutional Neural Network

This section describes the route-organizing procedure carried out by the suggested DCNN using the routing data collected from the aforementioned blockchain structure. The quantity of tokens moved, the time stamp, the number of tokens still present, and the location of the arrays through which the information passed constitute the total data the machine learning algorithm receives from the blockchain network. Here, a DCNN has been implemented to accurately choose the best route paths. 'Deep' refers to the convolution network layer. By performing the filter over the raw data and training the CNN to recognize harmful nodes, the feature map is produced. Conventional techniques, such as residual networks, neural networks and others, are used to identify routing paths that are congested, far away, or delayed. However, by taking into consideration the constantly changing, worldwide, and reliable routing information collected from the blockchain surroundings, the suggested DCNN is used to determine the routing connection in the correct way. This method comprises four steps for selecting the best routing links, including initialization, update, and selection and training stages (Figure 3).

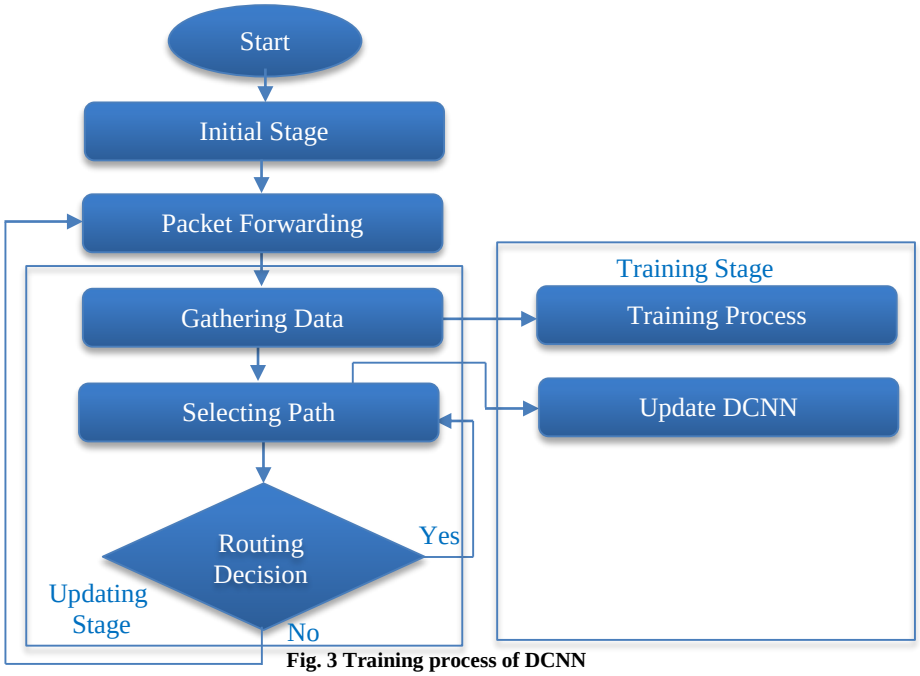

Fig. 3 Training process of DCNN

1st Stage: Initialization

Consider that there are $'n'$ routers that consist of a source node N_S, a destination node N_d, and a regular node N_r. Every router is required to provide a few different ways to get to the destination (R_d).

Based on each path's separation, value, and hop count, a queue (minimum priority) has been established for all routes.

For the sake of simplicity, let's take into consideration of a router. N_S with a set of potential paths $P = \{p1, p2, \ldots, p3, p4, \ldots pn\}$. From this collection of the set, the best routes are selected by applying the DCNN structure.

2nd Stage: Updating

At this stage, the routing choices have been corrected depending on the information gathered, the shortest hop path is chosen, and finally, the decision between all the routers is made. In this router, the CNN is trained using the least hop routing data, and an appropriate route is selected faster than traditional routing systems. To choose the best path for data transmission, the DCNN-based blockchain model appears to track network activity constantly and upgrade the routing path parameter values. Within a given time T, both the network traffic and the route information are modified. Every router can analyze the destination end's throughput, packet loss rate, and transmission latency before storing the data. The obtained

value increases the likelihood that the router intends to send the data packet effectively. Similarly, a shorter queue length raises the probability of efficient data transfer with no packet loss. Finally, a collection of updated training sets is optimum.

3rd Stage: Routing Decision and Path Selection

The basic goal of DCNN is to maintain track of any network traffic on the paths and to modify them when an invalid path to transport a data packet has been identified. The next neighbour path is going to be selected by the NN to confirm the existence of congestion, queue length, etc. Lastly, a viable route that won't cause congestion or take extra time to get there while avoiding packet loss is picked.

4th Stage: Training

The system is trained during the training stage, which also improves the updating phase routing choice and determines the congestion mode for every possible combination of c. Deep CNN develops after gathering the data during the upgrading stage, per the path's combination c. Learned DCNNs are utilized to make the routing decision during the update phase.DCNN provides more accurate and efficient routing decisions with less packet loss. In order to tune the parameter of DCNN optimization is required, this paper uses the BES algorithm for tuning the DCNN parameter. The following section gives a brief summary about the BES optimization algorithm.

2.2. BESO Algorithm

BES is a brand-new meta-heuristic optimization method that gets inspiration from nature and mimics bald eagle prey hunting behaviour. There are 3 stages to this technique. The bald eagle selects the optimal location, which is the quantity of food during the initial stage (selecting space). The eagle looks for prey within the defined region during the 2nd stage of its search (hunting in space). The eagle swings from the optimal location acquired in the 2ndstage to the ideal hunting location in the 3rd stage (swooping).

2.2.1. Space Selection

At this point, new positions are going to be established via the equation below.

$$P_{new}(i) = P_{best} + a.r(P_{mean} - P(i)) \quad (1)$$

Where P_{best} the optimal location is achieved, P_{mean} is the average location, and r is a random number, $P_{new}(i)$ is the $i-th$ entirely produced location, and P_{best}, is the finest position achieved. Every new position's fitness will be assessed, and if a new position (P_{new}) offers a superior fitness than that offered by the P_{best}, that new location is chosen as the P_{best},

2.2.2. Searching in Space

This method adjusts the location of eagles within this search space while assuming the suitable search space (P_{best}). The formulation of the upgrading model is as described below:

$$P_{new}(i) = P(i) + y(i).P(i) - P(i+1)) + x(i).(P(i) - P_{mean}) \quad (2)$$

Where $P_{new}(i)$ denotes the $i-th$ currently produced location, P_{mean} is the mean location, and $x\ and\ y$ denotes the direction of the $i-th$ position correspondingly.

$$\begin{cases} x(i) = \frac{xr(i)}{\max(\lvert xr \rvert)} : xr(i) = r(i).\sin(\theta(i)) \\ y(i) = \frac{yr(i)}{\max(\lvert yr \rvert)} : yr(i) = r(i).\cos(\theta(i)) \\ \theta(i) = a, \pi, rand; r(i) = \theta(i).R.rand \end{cases} \quad (3)$$

Where Ra parameter in the range is used to define the number of search cycles, and a is a control variable that determines the angle among point searches in the centre of the field, taking value in the range [5, 10]. The new location's fitness value is evaluated, and the P_{best} value adjusted in accordance with the outcomes.

2.2.3. Swooping

Using the best possible location, eagles move towards their intended prey during this phase. The following is how the hunting model is provided:

$$P_{new}(i) = rand.\ P_{best} + x1(i).(P(i) - C_1.P_{mean}) + y1(i).(P(i) - C_2.\ P_{best}) \quad (4)$$

Where $x1\ and\ y1$ are directional dimensions and $C_1\ and\ C_2$are random values [1, 2] it can be described as,

$$\begin{cases} x1(i) = \frac{xr(i)}{\max(\lvert xr \rvert)} : xr(i) = r(i).\sin(\theta(i)) \\ y1(i) = \frac{yr(i)}{\max(\lvert yr \rvert)} : yr(i) = r(i).\cos(\theta(i)) \\ \theta(i) = a, \pi, rand; r(i) = \theta(i) \end{cases} \quad (5)$$

This technique is shown in Figure 4 to make it easier to see and understand. $Npop$Represents the population size, and $MaxIter$ represents the maximum number of iterations. The shortest routing path was successfully determined using DCNN optimized BES algorithm.

3. Results and Discussion

The recommended BES-optimized DCNN routing scheme's effectiveness assessment and evaluation are examined here.

By contrasting it to traditional routing and meta-heuristic techniques like PSO and SSO-DCNN, as well as metrics like drop, delay, energy consumption, latency and throughput overhead, the effectiveness of the IoT-based Blockchain routing approach is verified by the presence of threatening nodes.

The obtained outcomes show that the proposed method is highly effective than conventional approaches such as PSO [21] and SSO-DCNN [21]. Table 1 describes the parameters for the suggested IoT-based blockchain technology system.

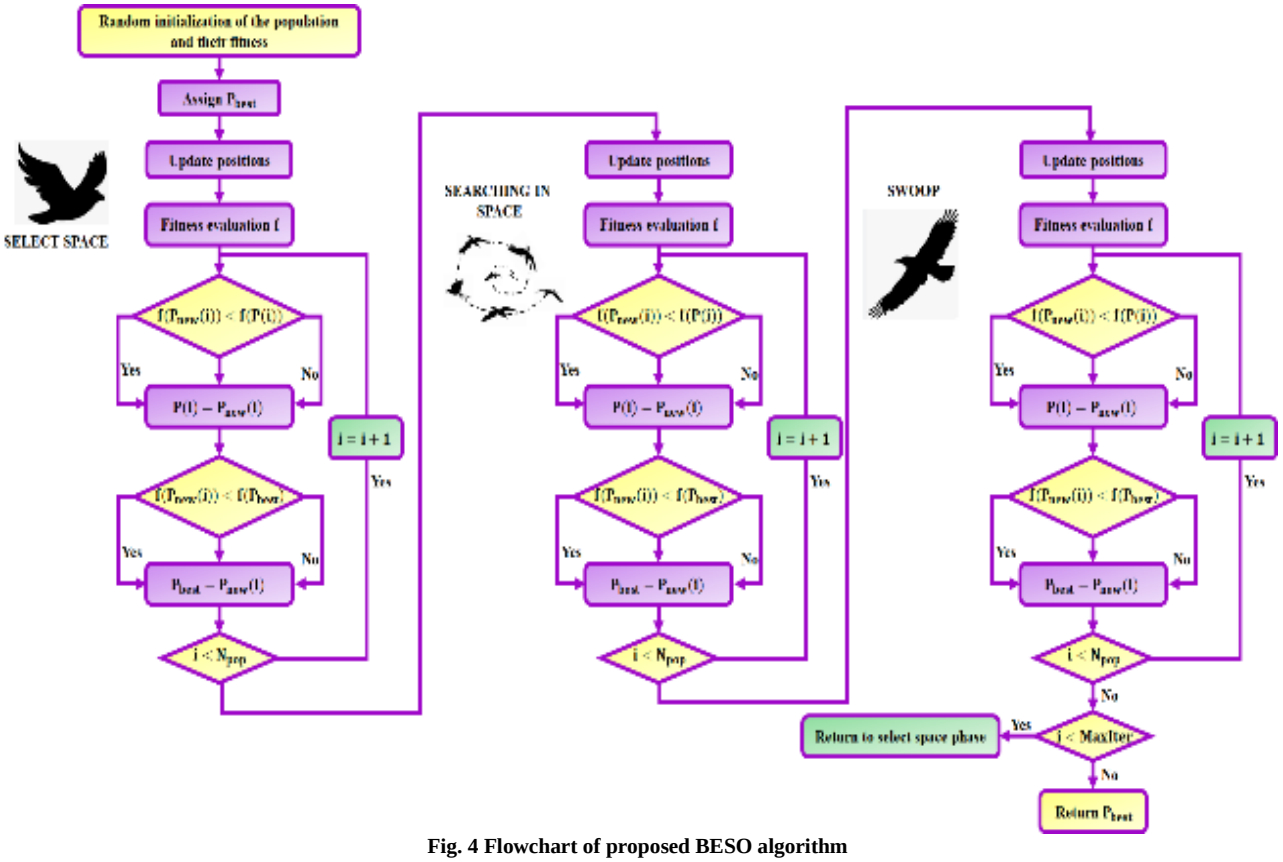

Fig. 4 Flowchart of proposed BESO algorithm

Table 1. Parameter description

Parameter	Size
RAM	16 GB
Simulator	NS2
CPU	2.6 GHz
Storage	16GB
Blockchain	5s

3.1. Packet Delay

Figure 5 compares the overall duration of the proposed BESO-DCNN method to those of PSO and SSO-DCNN. The graph demonstrates that other optimization methods lag behind the BESO-DCNN approach significantly. The BESO-DCNN technique is superior to the other protocols because it delivers packets to their destinations faster**.**

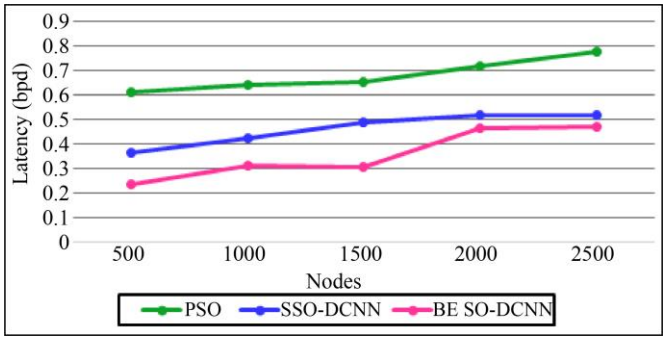

Fig. 5 Packet delay

3.2. Average Delivery Ratio

Figure 6 compares the proposed BESO-DCNN with PSO and SSO-DCNN-based blockchain routing techniques in the presence of harmful nodes regarding average packet delivery ratio. As a result, the average delivery ratio for the suggested BESO-DCNN-based PoA BC routing method is strengthened, and likewise, for different numbers of nodes, the BESO-DCNN technique performs much better than the PSO and SSO-DCNN.

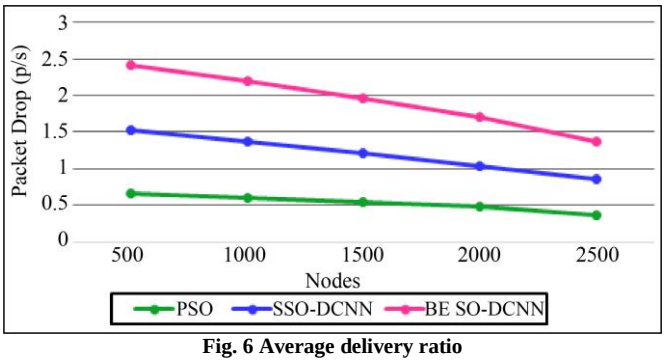

Fig. 6 Average delivery ratio

3.3. Packet Drop Ratio

In the appearance of unauthorized nodes, Figure 7 analyses the packet drop of the recommended BESO-DCNN with PSO and SSO-DCNN-based BC routing techniques.

Therefore, compared to the PSO and SSO-DCNN-based blockchain routing method, the suggested BESO-DCNN exhibits a lower packet drop with a notable improvement.

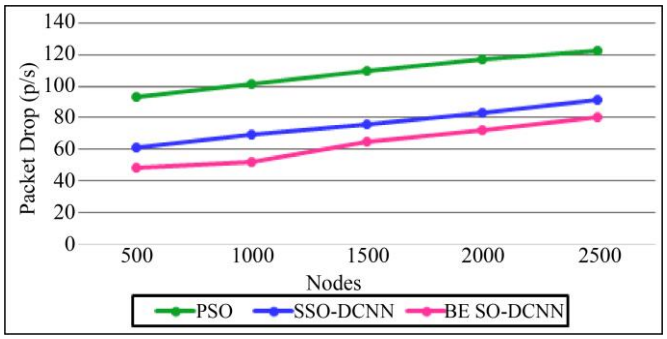

Fig. 7 Packet drop ratio

3.4. Energy Consumption

The total amount of energy a network uses to transfer packets among nodes is referred to as energy consumption. Figure 8 compares the PSO and SSO-DCNN algorithms with a proposed BESO-DCNN method. The line graph demonstrates that the SSO-DCNN algorithm consumes maximum energy than the other methods. However, the BESO-DCNN algorithm reduces the routing protocol and energy usage to a certain extent. When compared to all the other protocols, the BESO-DCNN algorithm uses the least amount of energy. In comparison to previous protocols, the suggested algorithm is more effective.

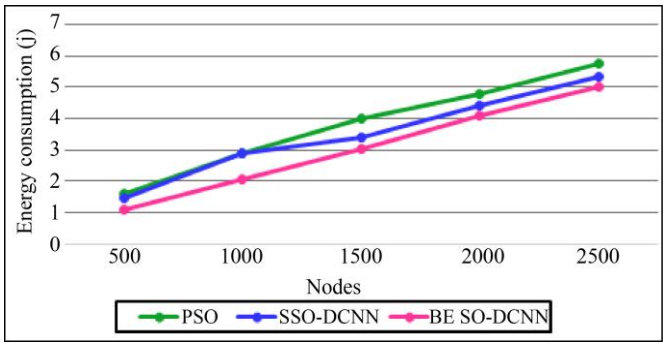

Fig. 8 Energy consumption

3.5. Average Latency

The latency of a network using blockchain technology is the interval among the submission of a transaction and the network's verification of that, while the latency of a swap is the interval during which the network processes the transaction.

Figure 9 illustrates the comparison of average latency analysis. From the graph representation, it is clear that the proposed algorithm achieves lesser latency compared to the other two approaches, i.e. PSO and SSO-DCNN. Thus, the suggested BESO-DCNN is more effective than other protocols.

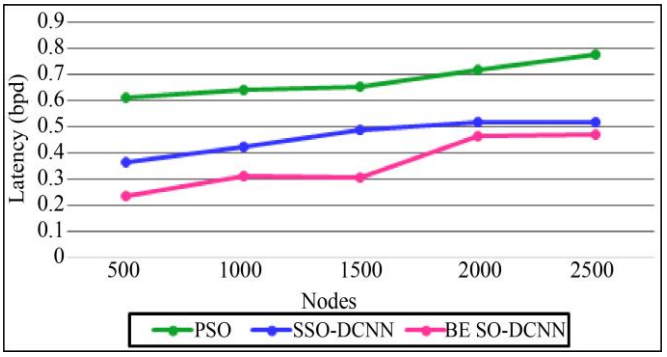

Fig. 9 Average latency

3.6. Throughput

The throughput evaluation of the proposed BESO-DCNN algorithm is shown in Figure 10, along with conventional approaches such as PSO and SSO-DCNN. The graph clearly shows that the proposed approach significantly increases throughput compared to the protocol.

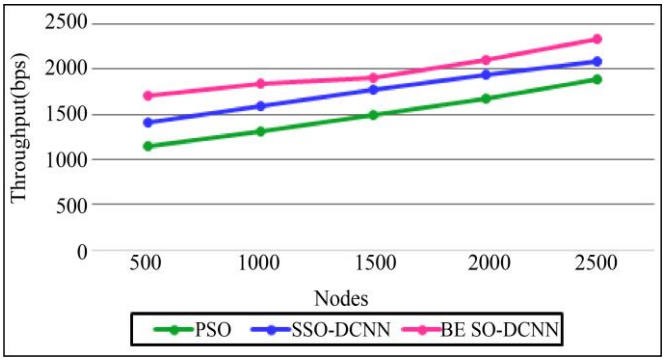

Fig. 10 Throughput

3.7. Overhead

The overhead evaluation of the suggested BESO-DCNN with PSO and SSO-DCNN-based BC routing scheme is shown in Figure 11. The suggested technique's average overhead is 1000 p/s, compared to the other two techniques, with an average overhead of 1200 p/s and 1400 p/s.

The BESO-DCNN-based PoA blockchain routing system is significantly better in moving packets, and it replicates with network circumstances in the routing surroundings, according to the aforementioned evaluation of performance.

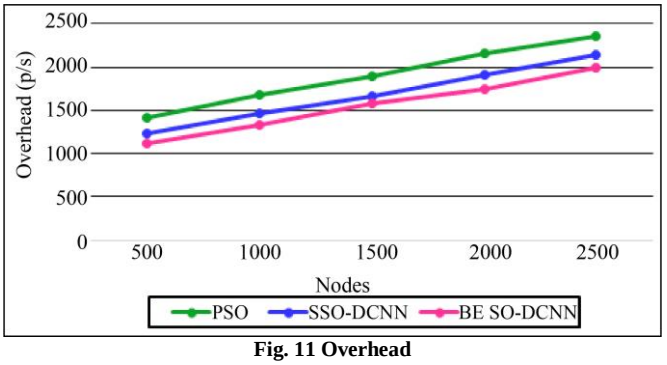

Fig. 11 Overhead

4. Conclusion

This research proposes an efficient routing technique based on BESO-DCNN and an IoT-based Blockchain distributed system framework. Each route is planned following the verification from the validator nodes, according to the PoA consensus Blockchain approach. The routing path and node information are collected by upgrading all of the information in the blockchain network's contracts without producing path traffic or harmful nodes. The DCNN technique makes routing decisions with the help of the BESO algorithm, selecting the best path from the DCNN findings. In addition, the suggested structure concentrates on the shortest and most energy-efficient routing chains with optimal decisions. At large network sizes, the suggested technique reduces routing overheads and communication expenses. Moreover, employing blockchain technology enables safe and dependable data routing. The attained outcomes clearly show that the proposed framework is more efficient than other conventional techniques.

References

[1] Jidian Yang et al., "A Trusted Routing Scheme using Blockchain and Reinforcement Learning for Wireless Sensor Networks," *Sensors*, vol. 19, no. 4, pp. 1-19, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] Sabir Hussain Awan et al., "BlockChain with IoT, an Emergent Routing Scheme for Smart Agriculture," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 4, pp. 420-429, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] Ibrahim A. Abd El-Moghith, and Saad M. Darwish, "Towards Designing a Trusted Routing Scheme in Wireless Sensor Networks: A New Deep Blockchain Approach," *IEEE Access*, vol. 9, pp. 103822-103834, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] M. Revanesh, and Venugopalachar Sridhar, "A Trusted Distributed Routing Scheme for Wireless Sensor Networks using Blockchain and Meta-Heuristics-Based Deep Learning Technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] Rekha Goyat et al., "A Secure Localization Scheme Based on Trust Assessment for WSNs using Blockchain Technology," *Future Generation Computer Systems*, vol. 125, pp. 221-231, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] Norah Saleh Alghamdi, and Mohammad Ayoub Khan, "Energy-Efficient and Blockchain-Enabled Model for Internet of Things (IoT) in Smart Cities," *Computers, Materials & Continua*, vol. 66, no.3, pp. 2509-2524, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Mohammed Amin Almaiah, *A New Scheme for Detecting Malicious Attacks in Wireless Sensor Networks Based on Blockchain Technology*, Artificial Intelligence and Blockchain for Future Cybersecurity Applications, Springer International Publishing, pp. 217-234, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Saba Awan et al., "Blockchain Based Secure Routing and Trust Management in Wireless Sensor Networks," *Sensors*, vol. 22, no. 2, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Khalid Haseeb et al., "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," *IEEE Access*, vol. 7, pp. 185496-185505, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Saba Awan et al., "Blockchain Based Authentication and Trust Evaluation Mechanism for Secure Routing in Wireless Sensor Networks," *Proceedings of the 15th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, Asan, Korea, pp. 96-107, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Hajra Zareen et al., "Blockchain and IPFS Based Service Model for the Internet of Things," *Proceedings of the 15th International Conference on Complex, Intelligent and Software Intensive Systems*, Asan, Korea, pp. 259-270, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Hao Liu et al., "Blockchain-Based Key Management and Green Routing Scheme for Vehicular Named Data Networking," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Shahid Abbas et al., "Securing Genetic Algorithm Enabled SDN Routing for Blockchain Based Internet of Things," *IEEE Access*, vol. 9, pp. 139739-139754, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Yuling Chen et al., "A Blockchain-Empowered Authentication Scheme for Worm Detection in Wireless Sensor Network," *Digital Communications and Networks*, vol. 10, no. 2, pp. 265-272, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Rajasoundaran et al., "Machine Learning Based Volatile Block Chain Construction for Secure Routing in Decentralized Military Sensor Networks," *Wireless Networks*, vol. 27, no. 7, pp. 4513-4534, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] Kuruva Lakshmanna et al., "Improved Metaheuristic-Driven Energy-Aware Cluster-Based Routing Scheme for IoT-Assisted Wireless Sensor Networks," *Sustainability*, vol. 14, no. 13, pp. 1-19, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[17] Tai-Hoon Kim et al., "A Novel Trust Evaluation Process for Secure Localization using a Decentralized Blockchain in Wireless Sensor Networks," *IEEE Access*, vol. 7, pp. 184133-184144, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Weizhi Meng, Wenjuan Li, and Liqiu Zhu, "Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1377-1386, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] M. Hema Kumar et al., "Real Time Two Hop Neighbour Strategic Secure Routing with Attribute Specific Blockchain Encryption Scheme for Improved Security in Wireless Sensor Networks," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, pp. 300-310, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] R.K. Yadav, and Rashmi Mishra, "An Authenticated Enrolment Scheme of Nodes using Blockchain and Prevention of Collaborative Blackhole Attack in WSN," *Journal of Scientific & Industrial Research*, vol. 79, pp. 824-828, 2020. [Google Scholar] [Publisher Link]

[21] M. Revanesh, and Venugopalachar Sridhar, "A Trusted Distributed Routing Scheme for Wireless Sensor Networks using Blockchain and Meta-Heuristics-Based Deep Learning Technique," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 9, 2021. [CrossRef] [Google Scholar] [Publisher Link]