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

Traitement du Signal
Vol. 43, No. 3, June, 2026, pp. 1155-1171
Journal homepage: http://iieta.org/journals/ts

Trust-Aware Secure Routing in Wireless Sensor Networks Using HSCRNet-Based Trust Prediction and FAABO Optimization

Palani Kumar Ramanathan[1*], Asokan Ramasamy[2]

[1] Department of Information Technology, Kongunadu College of Engineering and Technology, Trichy 621215, India
[2] Department of Electronics and Communication Engineering, Kongunadu College of Engineering and Technology, Trichy 621215, India

Corresponding Author Email: palanikumar@kongunadu.ac.in

https://doi.org/10.18280/ts.430307

Received: 14 April 2026
Revised: 16 June 2026
Accepted: 24 June 2026
Available online: 30 June 2026

Keywords:
trust-based routing, Wireless Sensor Networks, secure routing, deep learning, optimization algorithm

ABSTRACT

One of the challenging tasks in Wireless Sensor Network (WSN) is secure data transmission. Between the source and the corresponding target node, the transmission takes place by the specified path based on the routing information. From the remote location, the WSN can control and monitor the physical environment with high accuracy. There is a group of small nodes in the sensor network, which are inexpensive and tend to gather and disseminate critical data. In addition, the inexpensive nature of the various computational constraints and energy used by the sensor nodes along with the deployment of the ad hoc model. These deficiencies are resolved by several considerable types of research through minimum energy consumption protocol. While determining other factors, the huge impact created by the route selection strategy to enhance the lifetime of the sensor that followed the network lifetime. This is tackled by implementing the trust management scheme by generating trust relations among the sensor nodes. Hence, this work presents an optimal route selection framework with a trust factor as a base for improving the security of the WSN. Initially, the trust value of the node is predicted using the Hybrid Serial Cascaded Residual Network (HSCRNet) which is designed by connecting the Temporal Convolution Network (TCN) with Capsule Network in a serial manner. The prediction of trust value is used for mitigating malicious activities and performing secure data transmission in the WSN. After that, optimal path selection is performed using the Fitness Augmented African Bison Optimization (FAABO) Algorithm while considering the objective constraints like delay, energy, trust, throughput, link availability, link scalability, and packet delivery ratio (PDR). The optimal routing approach is considered a promising model for handling the energy consumption within the network. Finally, experimental validation is conducted to find the performance of the developed model. The proposed framework was evaluated in a MATLAB 2020a environment using WSN topologies containing 50–200 sensor nodes under malicious-node scenarios. HSCRNet utilizes node position, bit error rate (BER), traffic volume, link characteristics, and network topology features to classify trusted and malicious nodes. The dataset was divided into 70% training, 15% validation, and 15% testing samples. The classified trusted nodes are subsequently used by the FAABO routing algorithm for secure path selection. Experimental results show that HSCRNet achieved 98.84% classification accuracy, while FAABO improved routing trust, packet delivery ratio, throughput, and link availability compared with GOA, YSGA, CWO, and ABOA. The proposed method effectively mitigates malicious routing behavior and reduces energy consumption during secure data transmission.

1. INTRODUCTION

Wireless Sensor Network (WSN) is considered to be the game changer for the network industry, where the usage of wireless technology is more efficient for determining the extensive level of connectivity [1]. There is multitudinous sensor nodes combined to form the WSN, which are considerably less expensive and power with minimal characteristics. For collecting the relevant information, these nodes are responsible for targeting areas and data in the base station [2]. The particular information is gathered by the WSN and sensed by them in the specified region and communicates the readings to the base station [3]. Before the process of decision-making, the data is analyzed in the base station for different applications. There are repeaters in the WSN sensor nodes that help to transfer the data to other sinks or sensors [4]. In general, the energy consumption is performed in two ways node utilization for data transfer and detecting the environmental parameter. In WSN, the number of sensor nodes becomes the part based on the increased network size [5]. A lot of popularity is gained by efficient routing to maintain network scalability [6]. Most of the research attention is gathered by the WSN than the wired network, which also has more challenges in routing protocol because of the unreliable nature and channel interference in the transmission medium [7]. In addition, the WSN has some complexities like data integrity, data security and energy efficiency. In general, most of the sensors are battery-powered and it is considered to be a difficult task [8].

There is a requirement of energy efficient data transfer for enhancing the network lifetime by broadcasting the data from the sensors to the base station [9]. In general, the nodes are grouped by involving the clustering model to reduce the usage of electricity. The real-world environment is detected by the cluster member and pointed to the cluster head [10]. Various data dissemination protocols are utilized in the existing researchers to present the secure routing with the mobility modelling to enhance the system. In the node distribution, several hops are required in the base station for data collection and transmission [11]. Some of the security risks in WSN are attacks on integrity, authenticating, network availability and confidentiality. The routing information is disrupted by malicious behavior in the data transmission phase with the designated path [12]. Bio-inspired optimization algorithms are generally utilized in the previous literature for clustering [13]. In addition to that, other optimization algorithms called mayfly optimization, particle swarm optimization and genetic algorithms are adopted.

Based on Artificial Intelligence (AI), a beam-based heuristic algorithm is developed and it is supported to optimize the corresponding results [14]. However, the existing text-based security model also has some challenges, in which it is not able to perform different types of attacks simultaneously and it slows down the detection process. In addition to this, high energy consumption is required for performing the maliciousness [15]. Moreover, for securing the data encryption-based model is developed in the literature works, but it takes more memory storage and reduces the network energy [16]. In addition to this user details are exposed to the network which tends to security vulnerability. Within the minimal period, the malicious attack is detected through the earlier transaction and tends to packet loss [17]. Hence it is important to develop an intelligent model to perform effective communication through the secure routing strategy in the WSN network.

The below are the major contributions of this study:

1. To develop an effective communication strategy in WSN by integrating the trust and security mechanism with the optimal routing using deep learning and heuristic algorithm. This mechanism evaluates the shortest and most trusted path between the nodes to provide better communication in a realistic environment.

2. To present a Hybrid Serial Cascaded Residual Network (HSCRNet) model for performing the trusted node prediction to increase the security measures and it further helps in the efficient routing. The framework is the combination of the standard Temporal Convolution Network (TCN) and CapsNet, which is serially cascaded to mitigate malicious activities.

3. To design a Fitness Augmented African Bison Optimization (FAABO) algorithm for achieving the optimal routing in WSN for secure and efficient communication. The FAABO is the improved version of ABOA that provides the optimal solution by tuning the shortest path between the trusted nodes within the topology of the network.

The balance of the work is organized below. Section II describes the review of the conventional technique of inefficient routing. Section III presents the security issues in WSN and the proposed mechanism. Section IV defines the trust prediction model for efficient routing. Section V showed the optimal routing and its objective functions. Section VI deliberates the result and the simulation setup. Section VII illustrates the conclusion.

Although existing trust-aware routing protocols improve network security, several limitations remain. First, trust estimation is often based on static or rule-based mechanisms that cannot effectively capture temporal node behavior variations. Second, existing routing approaches optimize only one or two objectives, resulting in suboptimal performance when trust, energy consumption, delay, throughput, and packet delivery ratio must be jointly considered. Third, most methods evaluate performance under generic malicious conditions without explicitly addressing blackhole, wormhole, and Sybil attacks. Furthermore, many optimization-based routing approaches suffer from premature convergence and poor scalability when network size increases. To address these limitations, this work introduces HSCRNet for temporal trust prediction and FAABO for multi-objective secure routing optimization.

2. EXISTING WORKS

2.1 Related works

In 2022, Bin-Yahya et al. [18] initiated the routing protocol for enhancing the trust and energy efficiency in WSN using the adaptive algorithm. The new framework was developed to tackle the general routing attack. The filtering mechanism and the adaptive penalty factor were used to determine the values and volatilization. Based on the cluster head, the optimal secure routing was performed by the adaptive algorithm.

In 2020, Xu et al. [19] introduced the heuristic-based secure routing protocol for achieving efficient performance in the WSN network. The AI was utilized by the designed protocol to determine the intellectual and reliable scheme. The developed model achieved greater security to protect the data transmission with less complexity. The outcome from the simulation demonstrated that the designed protocol enhanced the network efficiency in dynamic scenarios.

In 2023, Yang et al. [20] presented the system using a quad-tree structure to minimize the complexity in the network management performance. The location and ID were determined to construct the authentication sensor using the encryption algorithm. This model avoids illegitimate sensor nodes to provide high security. The event metrics and time were considered to perform the cluster head selection to enhance communication. The generative algorithm was further used to secure the multi-path routing based on the hop count.

In 2024, Siddiq and Ghazwani [21] suggested the arithmetic encoding-based approach for the energy-efficient and secure WSN. The sensor node initialized after the WSN setup using the standard algorithm. The significant node feature was selected continuously to enhance the lifetime. The higher throughput achieved by the implemented model was revealed by the experimental findings.

In 2023, Salim et al. [22] adopted energy efficient and stable cluster selection using the advanced protocol in the WSN network. The random number generation was performed to stabilize the proposed work, which includes the CH selection using the node coverage. The finding revealed the energy-efficient performance achieved in the WSN by the adopted approach.

In 2023, Verma et al. [23] developed an innovative framework using Q-learning for secure routing. The optimized Q-learning and the unclonable function were utilized by the algorithm to ensure a reliable transmission path. The performance of the implemented algorithm was analyzed by conducting a performance analysis, which enhanced the filtering, and packet delivery ratio.

In 2024, Ahmed et al. [24] designed secure data transmission using the adaptive clustering model. The information was gathered initially based on the randomly placed nodes, which ensures the node's fair energy dissipation. The initiated protocol selected the cluster head and determined the intrusion detection to identify the presented malicious nodes in it. The malicious nodes were distinguished from the legal nodes based on the interference approach.

In 2022, Feng et al. [25] generated the multi-hop routing model in WSN using an advanced algorithm. The data transmission and the cluster head selection were included in this work for achieving the multi-hop routing. For the cluster head, the sensor nodes were sent the information, and it was further transmitted through the base station for the optimal hop selection. The trust model was introduced to perform the security-aware multi-hop routing.

Table 1. Comparative analysis of existing secure routing approaches in Wireless Sensor Networks (WSNs)

Author	Method	Metrics	Strength	Limitation
Han et al. [1]	Adaptive Trust Routing	Trust, Energy	Improves trust and energy efficiency	Limited dynamic trust adaptation
Haseeb et al. [2]	Heuristic Secure Routing	Throughput, Security	Low complexity	Limited attack analysis
Prasad and Periyasamy [3]	Authentication-Based Routing	Authentication Accuracy	Strong node verification	Increased computation
Rhesa and Revathi [4]	Arithmetic Encoding Routing	Throughput, Lifetime	Improves network lifetime	Limited scalability evaluation
Suresh and Prasad [5]	Cluster-Based Routing	Energy, Stability	Efficient CH selection	Uneven load distribution
Li et al. [6]	Q-Learning Routing	PDR, Reliability	Adaptive route selection	High computational overhead
Tabbassum and Pathak [7]	IDS-Based Clustering	Detection Rate	Effective malicious node detection	Additional processing cost
Vinitha et al. [8]	Trust-Based Multi-Hop Routing	Security, Routing Efficiency	Secure routing decisions	Optimization complexity

Note: WSNs: Wireless Sensor Networks; IDS: Intrusion Detection System; CH: Cluster Head; PDR: Packet Delivery Ratio; QoS: Quality of Service; IoT: Internet of Things.

Table 1 demonstrates that existing studies have significantly improved secure routing performance through trust management, clustering, optimization, and machine-learning-based approaches. However, most methods focus on either trust estimation or routing optimization independently. Furthermore, limited attention has been given to simultaneously handling multiple routing attacks while optimizing trust, throughput, delay, packet delivery ratio, scalability, and energy consumption. These limitations motivate the development of the proposed HSCRNet–FAABO framework.

2.2 Research gaps and challenges

Although several trust-aware and secure routing approaches have been developed for WSNs, significant challenges remain unresolved. Existing methods primarily focus on either trust evaluation or routing optimization independently, resulting in limited overall network performance. Most routing schemes fail to simultaneously optimize trust, throughput, scalability, packet delivery ratio, delay, and energy consumption. Furthermore, several existing trust models rely on static trust estimation mechanisms that cannot effectively capture temporal node behavior variations.

Another limitation is that many routing protocols are evaluated only under generic attack conditions without explicitly considering blackhole, wormhole, and Sybil attacks. In addition, optimization-based routing algorithms frequently suffer from premature convergence and reduced exploration capability when network size increases. To address these limitations, this work proposes the HSCRNet model for temporal trust prediction and the FAABO algorithm for multi-objective trust-aware secure routing optimization in WSNs.

3. VIEW OF WIRELESS SENSOR NETWORK AND PRIVACY ISSUES RESOLVED BY PROPOSED MECHANISM

3.1 Topological view of Wireless Sensor Network

WSN [26] is constructed by deploying a huge amount of wireless sensors to monitor the environment, system, or physical condition, which is arranged in an ad-hoc manner. The onboard processor is added along with the sensor nodes to maintain the specific target in the corresponding region. The base station is connected to the WSN based on the internet to share data and for communication [27]. WSN has been utilized for analyzing, processing and securing the data. There are three main layers in WSN network. The nodes are connected to the base station through a physical layer that helps to attain the physical communication. The reliable connection is ensured by the data link layer, which maintains the data transmission and performs effective communication. The specific data is communicated to the base station from the sensor nodes in the application layer. Here the data formation is determined by implementing the protocol, which also helps in the transmission and receiving [28]. The seamless operation is performed by facilitating the layers together in the WSN.

Different network topologies have been organized in WSN based on the corresponding application and the network type. The nodes are arranged in a hierarchical structure in the tree topology, in which the data is transferred between the nodes along different branches. WSN is considered to be a valuable network that ensures effective data collection and efficient monitoring for several applications. In addition, wireless communication ensures the flexible reconfiguration and deployment of the network. The basic structure of the WSN framework is shown in Figure 1.

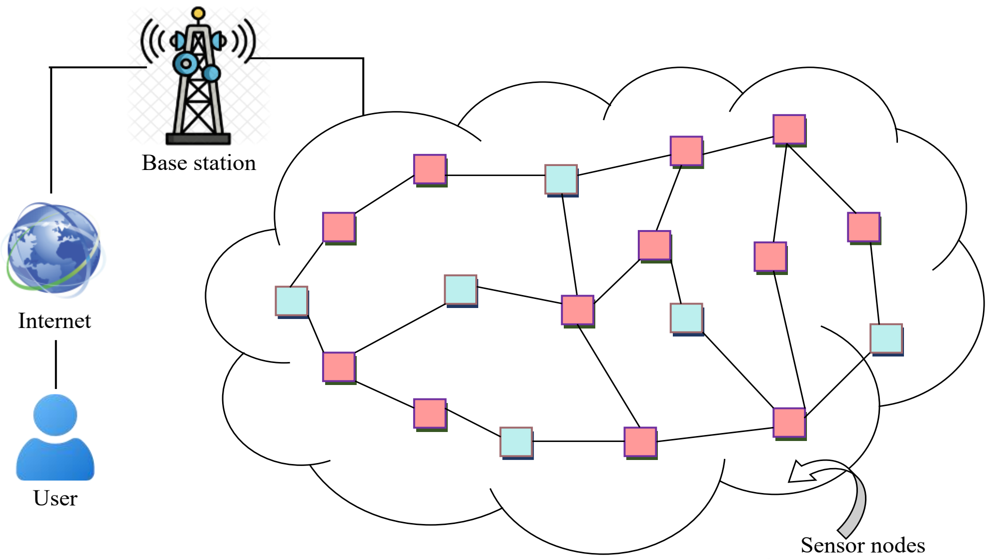


Figure 1. Illustration for the general Wireless Sensor Network (WSN) structure

3.2 Security issues in network

WSN [29] are generally vulnerable to different types of security threats, which affect the integrity, availability and confidentiality of the data. Some of the common issues faced by the WSN in reserving security are detailed below.

•Based on the strict resource constraints, WSN poses a limitation on the individual sensors. Storage and the computational limitation generated by the underlying energy constraints tend to new design issues.

•Because of the channel error, the packets may get affected in the wireless medium and cause conflict in the network. Without much effort, the denial-of-service (DoS) attack is launched by the attackers.

•The network faces greater latency because of the node processing and network congestion in the multi-hop routing. This tends to complexity in attaining synchronization among the sensor nodes.

•In the network, the tiny nodes are deployed on a large open scale. This tends to accidental node failure and causes potential issues for the physical capture. Due to these constraints, it is difficult to get secure data from harsh environments.

Based on the understanding of these issues, WSN provides a way for developing the secure sensor network.

3.3 Explanation of developed trust-based routing scheme in Wireless Sensor Network

The WSN is developed by comprising the sensor nodes, which are tiny devices deployed in the geographical area for environment sensing. This tends to collect data and communicate them. Through the wireless link, the intermediate nodes are connected. Therefore, it is necessary to have a suitable routing protocol for transferring the information in the network based on the presented different nodes. The data is transmitted through each sensor node in the multi-hop routing path. Intelligent decision making is necessary to reduce energy usage based on the clustering and rules. The secure routing protocol is known to be one of the challenging issues, because of the presence of malicious nodes in WSN. Therefore, the trust-based secure routing strategy was developed, in which it functioned by performing the authentication mechanism. This process includes effective key generation to offer improved security. Various researchers developed different methods for key management in authentication. Most of the trust computation models generally utilize the present and past behaviour of the nodes. Therefore, the new secure routing protocol is designed to perform effective authentication-based trust modelling with high-level security. Figure 2 defines the implemented intelligent framework for secure routing the WSN communication based on the heuristic-based hybrid model.

The new deep learning-based trust prediction framework and optimal routing mechanism are designed in this work to ensure efficient and secure communication in WSN. Two major key processes are implemented in this architecture which include the trusted node prediction and the optimal path selection. In general, the WSN is constructed with a greater number of sensor nodes that help to collect data from the corresponding environment. Between the base station and sensor node, the data link layer ensures a reliable connection to perform the data transmission. To perform secure communication, it is significant to guarantee the connected nodes, which transmit the data packet. Therefore, the selected nodes are to be trusted rather than malicious. Hence the new HSCRNet is developed for the trusted node prediction in WSN. Here the HSCRNet is the combined network, which includes the TCN and the CapsNet that cascaded serially to classify the nodes according to the characteristic. For this, the required attributes need to be given to the HSCRNet model. The attributes such as node position, Total Transmission Length, topology, and node name are input to the HSCRNet. Here, the TCN evaluates the sequential information from the given attributes based on the presented causal convolution layer in the network. The long-term dependencies are determined to learn the significant features. The result provides an effective feature, and it is given to the capsule network. The initial layer in the model extracts the lower feature based on the convolutional operation. The capsule layer detects each feature and provides the possible classification outcome. The HSCRNet classifies whether the nodes are trusted or malicious. Further, the trusted nodes are utilized in functioning the optimal routing to offer a trust-aware network. The trust-based efficient routing strategy is performed by selecting the shortest path among the trusted nodes to achieve efficient communication. Secure routing is handled to guarantee the network by selecting the optimal path selection. Here, the FAABO algorithm is implemented to optimize the shortest path. In addition, the multi-objective function is achieved by this optimal process, which ensures efficient routing. Based on this optimal routing, the data can be transmitted to the target destination with high security. In the end, the comparative assessment is carried out to determine the efficiency of the model.

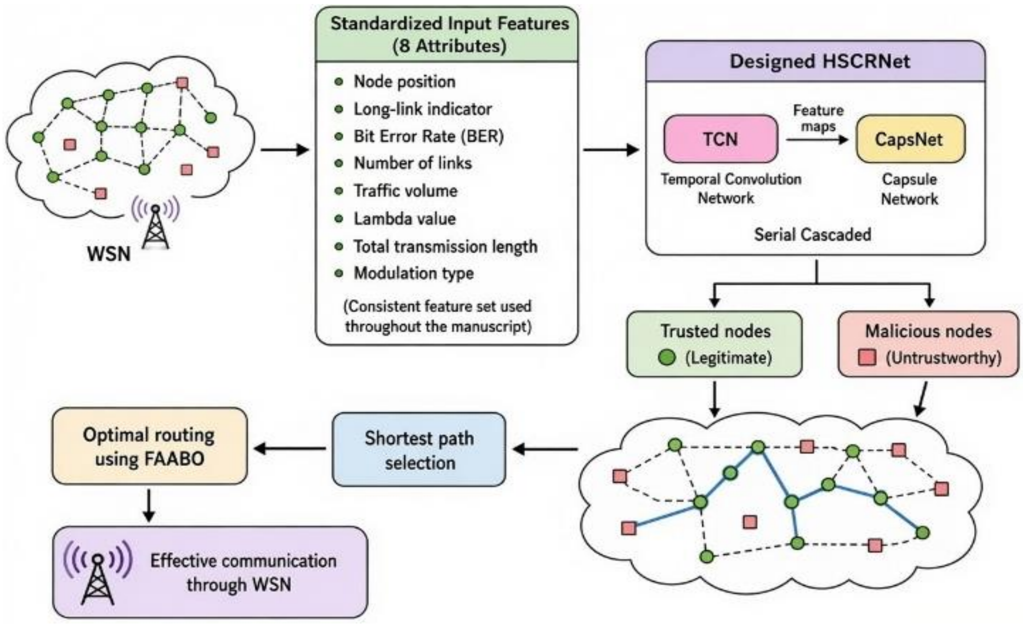


Figure 2. Illustration of proposed trust-based routing protocol in Wireless Sensor Network (WSN)

4. TRUST PREDICTION IN NODE USING HYBRID SERIAL CASCADED DEEP LEARNING NETWORK FOR ROUTING EFFICIENCY

4.1 Temporal Convolution Network

TCN [30] is a kind of convolution network that has three different modules in its structure called dilated residual and casual convolution. By using these convolution modules, the long-term features can be integrated. Here the result sequences $\hat{k}_0, \ldots, \hat{k}_T$ are predicted using the initial sequence of input $z_0, \ldots, z_T$. The prediction is generated by the input sequence model by utilizing Eq. (1).

$$\hat{k}_0, \ldots, \hat{k}_T = f(z_0, \ldots, z_T) \tag{1}$$

Here the model temporal sequence is evaluated based on the function f. The expected loss is minimized by the implementation of this function between the predicted and the actual result. The significant process of the TCN structure is to generate the outcome that corresponds to the length of the input and solve the leakage based on the presented casual convolution. The filter is adopted by the network to determine the larger region, where the length can be expanded. The original filter is expanded by adding the zero padding and it is formulated using Eq. (2).

$$F(v) = (Z * f)(v) = \sum_{i=0}^{m-1} f(i).Z_{v-d.i} \tag{2}$$

Here the term d indicates the dilation factor, $l$defines the convolution filter. The term $v-d$ is the earlier index measure. Further, the number of layers is analyzed to evaluate the complete coverage based on the receptive kernel derived from Eq. (3).

$$n = [(m-1)/(l-1)] \tag{3}$$

Here, n is considered to be the number of layers. There are multiple filters in each layer for performing the feature extraction.

4.2 Dataset preparation and training procedure

The trust prediction dataset was generated from simulated WSN environments containing trusted and malicious nodes. Each sample consisted of eight attributes: node position, long link indicator, bit error rate (BER), number of links, traffic volume, lambda value, total transmission length, and modulation type. All numerical features were normalized to the range [0,1] using min-max normalization. Trusted labels were assigned to nodes exhibiting packet forwarding ratios greater than 90% and normal communication behavior. Malicious labels were assigned to nodes performing packet dropping, route manipulation, or identity spoofing activities. A sliding time window of 20 communication rounds was used for feature extraction. The dataset was divided into 70% training samples, 15% validation samples, and 15% testing samples. Model training was performed using the Adam optimizer with a learning rate of 0.001 and a batch size of 32.

4.3 Capsule network

CapsNet [30] is a type of Artificial Neural Network (ANN) that is mainly developed to perform the duplication in the biological neural organization. One of the significant components in the network structure is the capsule layer. The main performance of this capsule layer is to affine the transformation with squashing and weighted sum. The affine transformer is more useful in determining the real orientation based on the feature obtained by the convolutional layer. The expression of the prediction vector is computed using Eq. (4).

$$\hat{g}_{z|j} = k_{jz}.g_j \tag{4}$$

Here, the term $\hat{g}_{z|j}$ is the predictive vector with the weight matrix k_{jz} . The resultant vector from the capsule is represented as g_j. The evaluation of the weighted vector is determined using Eq. (5).

$$w_z = \sum n_{j,k}\hat{g}_{z|j} \tag{5}$$

Here, the weighted sum is indicated as w_z with the coefficients $n_{j,z}$. The result is evaluated using Eq. (6).

$$g_j = \frac{||y_j||^2 y_j}{1 + ||y_j||^2 ||y_j||} \tag{6}$$

Here, $y_j \in Eb_{Ex}$ implies the input with the resultant representation $g_j \in wt_2$. Based on this, the system can evaluate the spatial relationship for the given input.

4.4 Training data generation and feature engineering

The trust prediction dataset was generated from simulated WSN environments containing both trusted and malicious nodes. The dataset was created by varying the network size from 50 to 200 sensor nodes under different communication conditions and attack scenarios. Each node record consisted of eight attributes, namely node position, long-link indicator, bit error rate (BER), number of links, traffic volume, lambda value, total transmission length, and modulation type. Prior to model training, all numerical features were normalized into the range [0,1] using min-max normalization to ensure stable convergence of the deep learning model. Trusted labels were assigned to nodes exhibiting normal packet forwarding behavior and forwarding ratios greater than 90%, whereas malicious labels were assigned to nodes performing packet dropping, route manipulation, selective forwarding, Sybil, or blackhole attack activities. A sliding temporal window containing 20 communication rounds was employed to capture sequential node behavior patterns. The generated dataset was divided into 70% training samples, 15% validation samples, and 15% testing samples. The HSCRNet model was trained using the Adam optimizer with a learning rate of 0.001 and a batch size of 32. The training process continued until convergence was achieved with minimum validation loss. The extracted temporal features from the TCN were subsequently provided to CapsNet for trusted-node classification. The diagram of the proposed HSCRNet for trusted node prediction is shown in Figure 3.

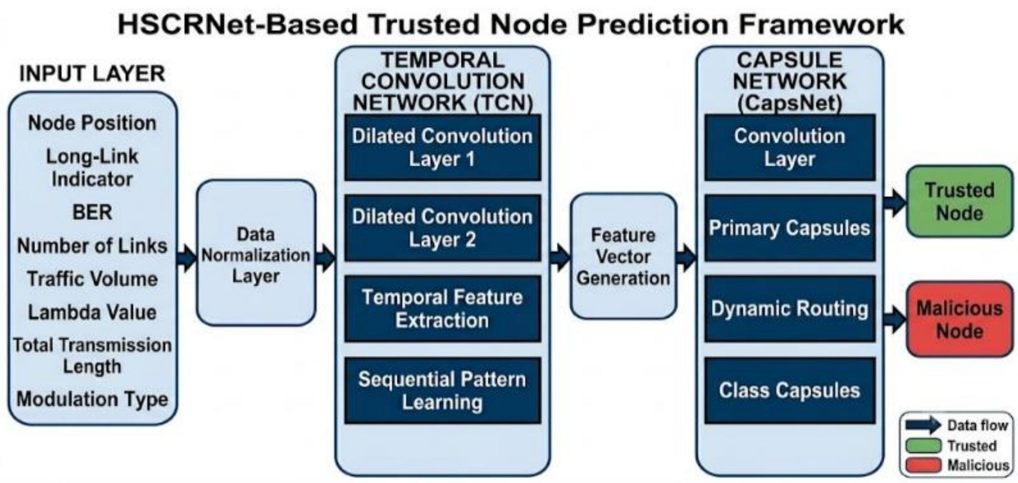


Figure 3. Detailed Hybrid Serial Cascaded Residual Network (HSCRNet) architecture for trusted and malicious node classification using communication and network features

5. IMPROVED OPTIMIZATION ALGORITHM FOR OPTIMAL ROUTING AND ITS OBJECTIVE FORMULATION IN TRUST-AWARE NETWORK

5.1 Fitness augmented-value of ABO

The designed optimal routing strategy utilizes the FAABO algorithm for selecting the trusted and shortest path in WSN communication [31].

Purpose: The implementation of FAABO is to select the shortest path in the WSN by providing the optimal routing solution. Here, the FAABO supports the selection of the shortest path based on the possible trusted nodes in the WSN framework. While transferring data, route optimization tends to minimize energy consumption and extend the network lifetime. In addition to this, it also enhances trust, scalability and throughput by providing the optimal path selection.

Novelty: The designed FAABO is an improved version of the conventional ABOA. ABOA is the nature-based metaheuristic algorithm that copies the survival characteristic of the African Bison. In addition to this, the ABOA algorithm also utilizes the eliminating, jousting and foraging behaviour. The competitive and superior behaviour is exhibited by the ABOA by maintaining the exploitation and exploration effectively [32]. The better individual is produced by the population, which tends the ABOA to attain the optimal value faster. It can solve real-world engineering problems than conventional algorithms. Also, it is considered to be a multi-objective optimization tool to process complex issues. However, it also has some complexities in performing the faster convergence for the long-term issues. To tackle this issue and to enhance the algorithm to generate the optimal solution, the random value in the baseline ABOA is replaced with the new value, which is based on the fitness function to develop the FAABO algorithm. The updated random value is evaluated using Eq. (7).

$$S = \frac{wgt - cgt + mgt}{bgt} - bgt \times \frac{-0.001 - 0.001}{wgt - bgt} - 0.001 \tag{7}$$

Here, the worst and the best fitness function is indicated as wgt and bgt. The current and mean fitness value is denoted as cgt and mgt. The term S is the replaced random value in ABOA in which its original value ranges between [-0.01, 0.01]. The new random value is updated in the exploration phase of ABOA, where it defines the jousting behavior and is defined in Eq. (8).

$$K = Y'_{ubest} - Y'_{ubest}\left(\frac{ran * Y'_j}{2}\right) * (cos(Y_i^t) + sin(Y_i^t)) * S \tag{8}$$

Here, the population-based fighting power of bison is indicated as K. The best individual position is specified as Y'_{ubest}. The pseudocode of the presented FAABO algorithm is given in Algorithm 1.

Ablation Analysis of FAABO

Three variants were evaluated:

1. Original ABOA
2. ABOA with Fitness-Based Random Update
3. Full FAABO

Algorithm 1. Implemented Fitness Augmented African Bison Optimization (FAABO)

```
Input: Nodes
Output: Optimal routing
Population generation
Evaluate the objective function
    While the iteration starts
      Update the random value S using Eq. (7)
          Calculate the foraging behavior.
          Determine the bathing behavior.
          Compute the jousting characteristic.
          Calculate the mating behavior.
           Eliminate the behaviour into two subgroups.
          Update the best position
    Save the best solution
  end while
Return to the optimal solution.
```

Table 2. Ablation study of Fitness Augmented African Bison Optimization (FAABO) and its components for convergence performance analysis

Method	Mean Fitness	SD	Convergence Iteration
ABOA	5.32	0.76	92
ABOA+Fitness Update	4.98	0.61	81
FAABO	4.65	0.58	72

Note: ABOA: African Bison Optimization Algorithm; SD: Standard Deviation.

The fitness-based update improved exploration capability by dynamically adapting the search behavior according to population fitness distribution. The modification reduced premature convergence and improved routing stability. Table 2 reports mean fitness, standard deviation, and convergence iteration for all variants.

5.2 Optimal routing and its mechanism

Based on the demand for an efficient and secured WSN, a trust-based routing protocol is developed in this work. Here the optimal routing protocol is achieved by implementing the FAABO algorithm.

Once the trusted nodes are selected, the path planning scheme is performed using the FAABO algorithm to attain the secure and shortest path selection based on the optimal routing. The routing procedure is more significant in the network to tackle the issues in the data transmission process. Various attacks prone to WSN, like wormhole attacks, blackhole attacks, and Sybil attacks, happened because of the remote and open deployment environment [33]. Hence, to guarantee the network, secure routing is performed by selecting the trusted nodes for the path selection. This process determines the most efficient route among the trusted nodes by selecting the path with less cumulative cost. This has been achieved by implementing an effective algorithm to calculate the shortest path within the topology of the network. The optimization process is used to attain the shortest path between the number of nodes in the WSN by using the FAABO algorithm [34]. The objective function for achieving the optimal routing is described in Eq. (9).

$$OF = \underset{\{Sp^n\}}{argmax}\left[Thp + Tst + Lka + Lns + Pdr + \frac{1}{Erc + Dly}\right] \tag{9}$$

To avoid scale differences among performance metrics, all objective variables were normalized into the interval [0,1].

$$Trust_{norm} = (Trust - Trust_{min})/(Trust_{max} - Trust_{min})$$

$$Throughput_{norm} = (Throughput - Throughput_{min})/(Throughput_{max} - Throughput_{min})$$

$$Energy_{norm} = (Energy - Energy_{min})/(Energy_{max} - Energy_{min})$$

$$Delay_{norm} = (Delay - Delay_{min})/(Delay_{max} - Delay_{min})$$

The final fitness function is formulated as:

$$Fitness = 0.25 \times Trustnorm + 0.20 \times Throughputnorm + 0.15 \times Availabilitynorm + 0.10 \times Scalabilitynorm + 0.10 \times PDRnorm - 0.10 \times Energynorm - 0.10 \times Delaynorm$$

The weights were selected after sensitivity analysis and maintained constant throughout all experiments.

Throughput is measured by the number of successful packets transmitted from the origin to the corresponding destination over time and it is computed using Eq. (10).

$$Thp = \frac{Q_s}{t} \times 100 \tag{10}$$

Here, the successful amount of transmitted packets is termed as Q_s and the time indicated as t.

Trust helps to evaluate the security of the implemented model in the process of routing. Trust is formulated based on

Eq. (11).

$$Tst = \{M^d + M^i + M^f + M^l\} \tag{11}$$

Here, the direct and the indicated trust are represented as M^d and M^i. Similarly, the term M^l and M^f denoted the integrity and the forwarding rate factor.

Link availability analyses the stable and available link selected by the sensor node in the designed network.

Link scalability analyzes the number of nodes that increased after establishing the WSN. It is considered to be an efficient routing protocol in WSN [35].

The packet delivery ratio helps to identify the attacks in the nodes based on tracking the node ratio. It is evaluated using Eq. (12).

$$Pdr = \frac{\rho^Y_{X(t_1,t_2)}}{\tau^Y_{X(t_1,t_2)}} \tag{12}$$

Here, the term $\rho^Y_{X(t_1,t_2)}$ denoted the total number of packets delivered from X node to Y node with corresponding time. The term $\tau^Y_{X(t_1,t_2)}$ is the total transmitted packet.

Energy consumption determines the average energy taken by each node within the simulation time and it is determined using Eq. (13).

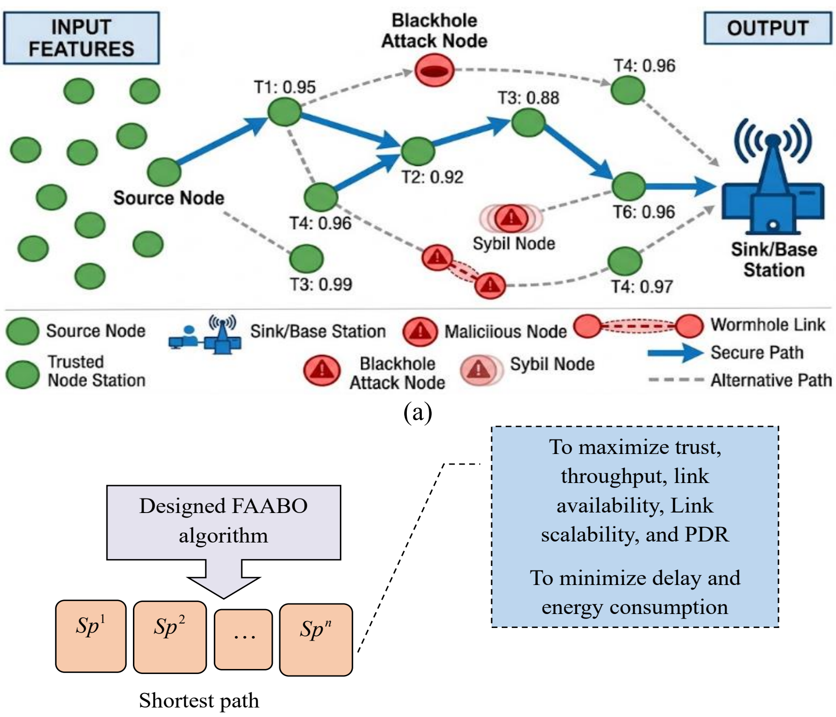
$$Erc = \grave{\eta} - \breve{\alpha} \tag{13}$$

Here, the initial and the remaining energy is specified as $\grave{\eta}$ and $\breve{\alpha}$.

Delay is determined based on the hop ratio needed for the total node routing contained in WSN and it is measured using Eq. (14).

$$Dly = \frac{zy}{n} \tag{14}$$

Here, n is the total number of presented nodes in WSN and zy is the total hop number required for routing.



(a)

(b)

Figure 4. (a) Node illustration, (b) solution encoding structure for designed Fitness Augmented African Bison Optimization (FAABO) algorithm

In the end, the best solution presented by the given optimization procedure is based on selecting the trusted nodes in the WSN system. The significant function of the trust-based routing protocol is to evaluate the efficient and trustworthy route between the two nodes, in which it can send data to the corresponding destination. The solution encoding diagram for the implemented optimal routing strategy using FAABO is defined in Figure 4.

6. RESULTS AND DISCUSSION

6.1 Experimental setup

The proposed framework was implemented and evaluated using MATLAB R2020a in a simulation environment covering an area of 1000 m × 1000 m. The network consisted of 50, 100, 150, and 200 sensor nodes randomly deployed within the simulation area, with the sink node positioned at the center (500 m, 500 m). Each sensor node was initialized with an energy of 2 J, and a First-Order Radio Energy Model was employed to estimate energy consumption during wireless communication. The transmission range of each node was set to 100 m, while the packet size was fixed at 512 Bytes. To evaluate the robustness of the proposed security framework, different network attack scenarios were considered by introducing 10%, 20%, and 30% malicious nodes implementing Blackhole, Wormhole, and Sybil attacks. The simulations were executed for 1000 rounds, and a random seed value of 42 was used to ensure reproducibility of the experimental results. Performance evaluation was conducted using metrics such as Packet Delivery Ratio (PDR), Throughput, End-to-End Delay, Packet Loss Ratio (PLR), Energy Consumption, Network Lifetime, Detection Accuracy, Precision, Recall, and F1-Score. All simulations were carried out on a system equipped with an Intel® Core™ i7 processor, 16 GB RAM, and Windows 10 (64-bit) operating.

6.2 Evaluation metrics

Accuracy, mean absolute error and mean absolute scaled error are evaluated using Eqs. (15), (16) and (17).

$$Acy = \frac{Tk + Ts}{Tk + Ts + Fk + Fs} \tag{15}$$

Here the term Tk and Ts denoted the true positive and negative. Similarly, the term Fk and Fs specifies the false positive and false negative respectively.

$$MAE = \frac{\sum_{i=1}^{z}(u_i - s_i)}{k} \tag{16}$$

$$MASE = \frac{1}{k}\sum_{i=1}^{z}\left(\frac{s_i - u_i}{s_i}\right) \tag{17}$$

Mean percentage error, root mean square error and symmetric mean absolute percentage error demonstrated using Eqs. (18), (19) and (20).

$$MEP = \frac{100\%}{k}\sum_{i=1}^{z}\left(\frac{s_i - u_i}{s_i}\right) \tag{18}$$

$$RMSE = \sqrt{\frac{\sum_{i=1}^{z}(u_i - s_i)^2}{k}} \tag{19}$$

$$SSMAPE = \frac{100}{k}\sum_{i=1}^{k}\frac{|u_i - s_i|}{\left(\frac{|u_i| + |s_i|}{2}\right)} \tag{20}$$

Here the observed and the predicted value is represented as u and s respectively.

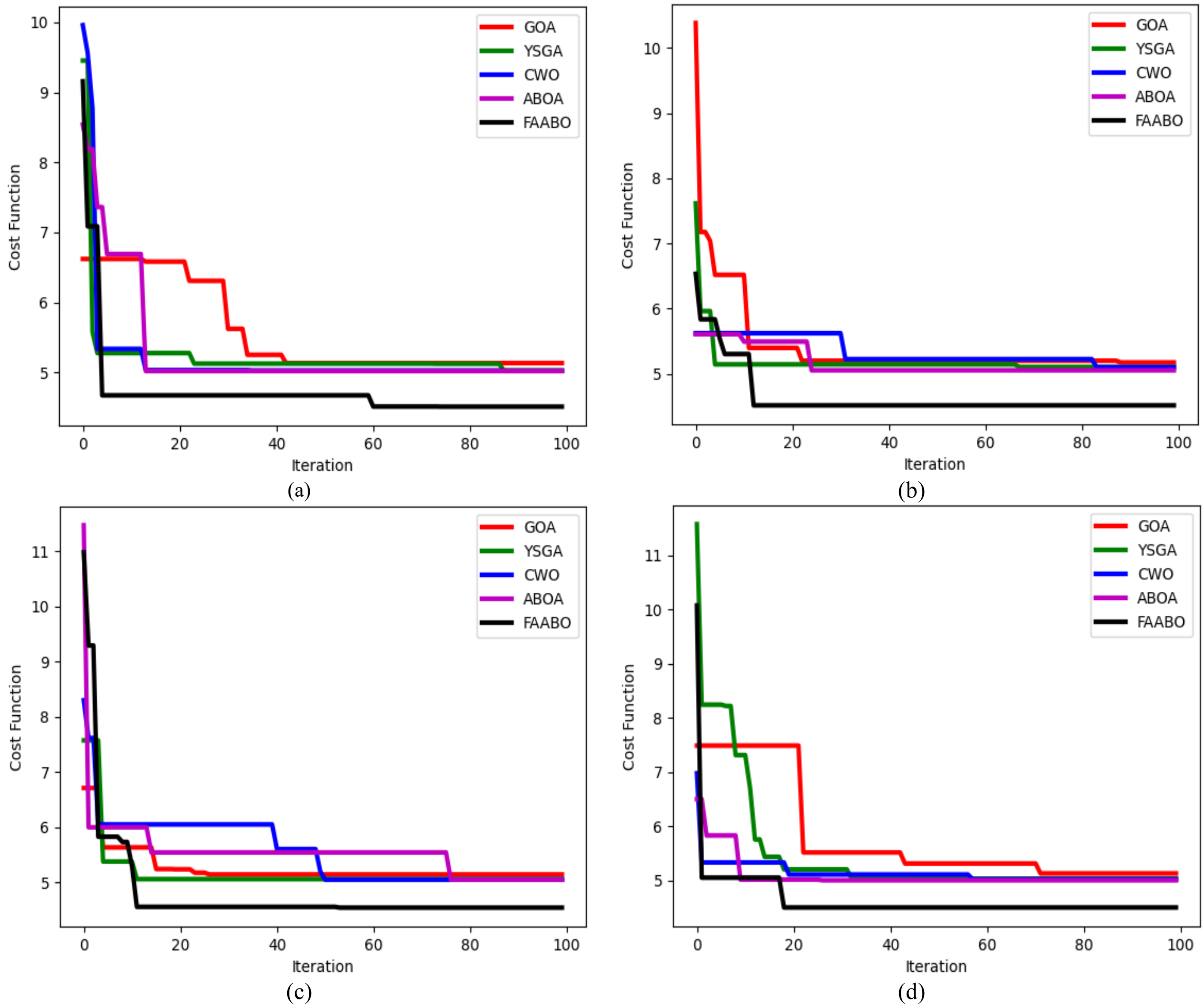
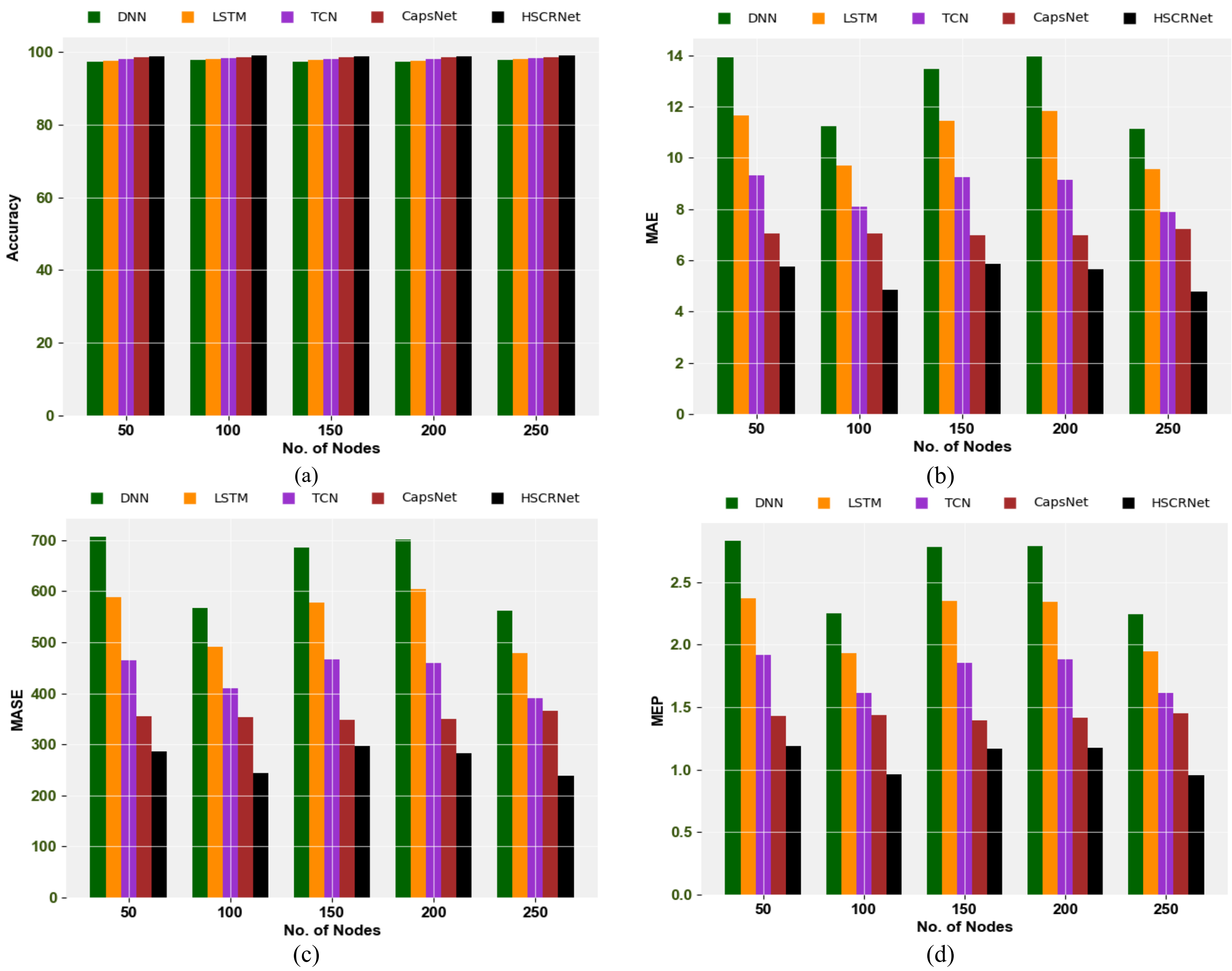


Figure 5. Convergence estimation of the designed Fitness Augmented African Bison Optimization (FAABO) algorithm differentiated from other conventional algorithms in terms of "(a) Node 50, (b) Node 100, (c) Node 150, and (d) Node 200"

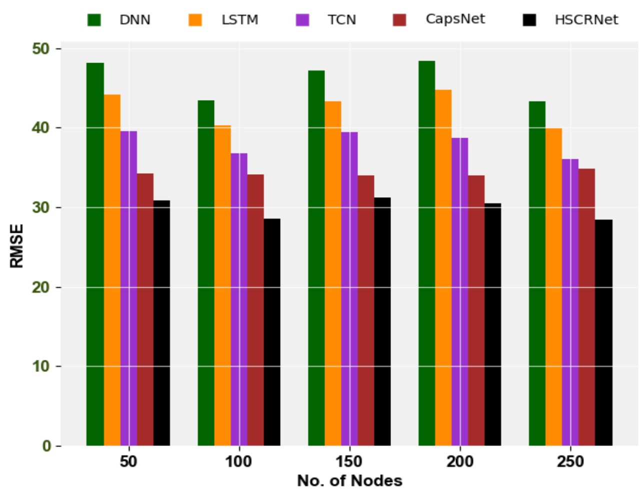
Table 3. Statistical determination of suggested Fitness Augmented African Bison Optimization (FAABO) algorithm compared with other traditional algorithms

Terms	GOA [33]	YSGA [34]	CWO [35]	ABOA [26]	FAABO
Node 50					
"Worst"	6.621197	9.45378	9.959265	8.539115	9.158044
"Best"	5.134928	5.030331	5.022451	5.021386	4.512297
"Mean"	5.581412	5.235163	5.192009	5.30036	4.726812
"Median"	5.134928	5.126775	5.028596	5.021386	4.674031
"Std"	0.630526	0.60869	0.756324	0.761218	0.619197
Node 100					
"Worst"	10.38419	7.614866	5.620727	5.606006	6.532778
"Best"	5.172463	5.103105	5.099206	5.0516	4.513546
"Mean"	5.419695	5.179182	5.32527	5.168745	4.644103
"Median"	5.199241	5.143145	5.223037	5.0516	4.513546
"Std"	0.67675	0.283526	0.202939	0.21026	0.375884
Node 150					
"Worst"	6.707096	7.570473	8.297102	11.47027	10.97799
"Best"	5.139441	5.055535	5.045083	5.044292	4.53857
"Mean"	5.264846	5.178429	5.550725	5.538989	4.799502
"Median"	5.139441	5.055535	5.115395	5.539313	4.552742
"Std"	0.33153	0.49497	0.617004	0.661442	0.956488
Node 200					
"Worst"	7.48668	11.57063	6.97678	6.499613	10.07004
"Best"	5.130031	5.033089	5.0225	5.003201	4.501915
"Mean"	5.780783	5.461969	5.130927	5.093146	4.651048
"Median"	5.312651	5.033089	5.1099	5.003201	4.501915
"Std"	0.916001	1.079548	0.215771	0.290615	0.582384

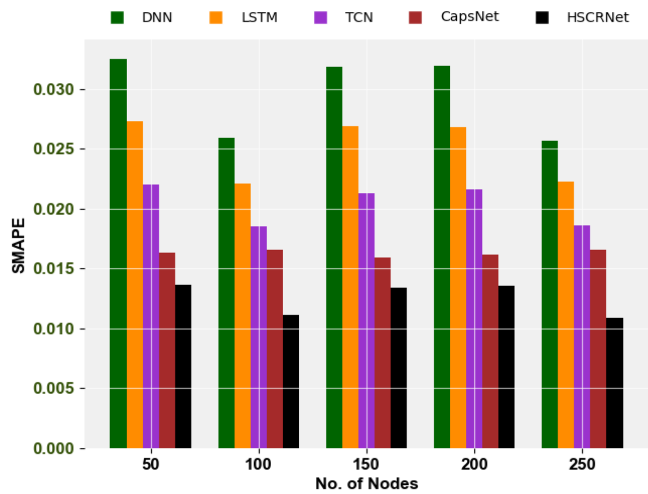
Note: FAABO: Fitness Augmented African Bison Optimization; ABOA: African Bison Optimization Algorithm; GOA: Grasshopper Optimization Algorithm; YSGA: Yellow Saddle Goatfish Algorithm; CWO: Carpet Weaver Optimization; SD: Standard Deviation.



(a) (b) (c) (d)



(e)



(f)

Figure 6. Performance comparison of HSCRNet-based trust prediction vs. other traditional techniques regarding: (a) Accuracy, (b) MAE, (c) MASE, (d) MEP, (e) RMSE, and (f) SMAPE

Note: HSCRNet: Hybrid Serial Cascaded Residual Network; MAE: Mean Absolute Error; MASE: Mean Absolute Scaled Error; MEP: Mean Error Percentage; RMSE: Root Mean Square Error; SMAPE: Symmetric Mean Absolute Percentage Error.

Table 4. Overall comparison of the suggested HDCRNet for trust prediction differentiated from other techniques

Optimizers	DNN [31]	LSTM [32]	TCN [29]	CapsNet [30]	HSCRNet
			MEP		
"Adam"	3.116051	2.627206	2.205098	1.705397	1.46944
"SGD"	2.987718	2.565283	2.086786	1.614622	1.384787
"RMSprop"	2.887935	2.469653	1.998015	1.530121	1.279
"Adamax"	2.852471	2.371811	1.887302	1.418746	1.182317
"AdaGrad"	2.813228	2.358073	1.89095	1.434313	1.177595
			SMAPE		
"Adam"	3.576839	3.008033	2.538297	1.951616	1.692784
"SGD"	3.425356	2.95271	2.394195	1.863226	1.586036
"RMSprop"	3.312612	2.833432	2.296947	1.75721	1.464058
"Adamax"	3.270864	2.725293	2.165847	1.628512	1.352711
"AdaGrad"	3.22461	2.721747	2.170309	1.652537	1.358422
			MASE		
"Adam"	760.1316	667.8181	542.5873	434.7147	355.8647
"SGD"	738.4942	630.3606	511.0496	407.9158	336.2368
"RMSprop"	711.0035	613.0363	482.7494	371.3618	328.3875
"Adamax"	726.5754	602.9267	488.5034	354.2456	291.0348
"AdaGrad"	714.238	572.5655	472.6876	355.1093	297.2649
			MAE		
"Adam"	15.06276	13.19432	10.77632	8.709936	7.16116
"SGD"	14.77149	12.34517	10.17147	8.042807	6.749668
"RMSprop"	14.14548	12.2144	9.639877	7.422103	6.538285
"Adamax"	14.38315	11.86302	9.59502	7.048535	5.819727
"AdaGrad"	14.12969	11.44881	9.34716	6.992102	5.9174
			RMSE		
"Adam"	49.67568	47.21882	42.34044	38.45736	34.55026
"SGD"	49.49064	45.12596	41.00658	36.73986	33.32904
"RMSprop"	48.6496	45.06246	39.97332	34.911	33.22924
"Adamax"	49.28542	44.69397	40.04944	34.15287	30.96761
"AdaGrad"	48.68652	43.31697	39.18099	34.13697	31.69988
			Accuracy		
"Adam"	96.96532	97.36013	97.83152	98.25782	98.57639
"SGD"	97.0617	97.52724	97.9672	98.39484	98.6509
"RMSprop"	97.16016	97.56875	98.06256	98.51161	98.69777
"Adamax"	97.1407	97.62884	98.09535	98.59239	98.83953
"AdaGrad"	97.17769	97.71731	98.13346	98.59561	98.81166

Note: DNN: Deep Neural Network; LSTM: Long Short-Term Memory; TCN: Temporal Convolutional Network; CapsNet: Capsule Network; HSCRNet: Hybrid Serial Cascaded Residual Network; MEP: Mean Error Percentage; SMAPE: Symmetric Mean Absolute Percentage Error; MASE: Mean Absolute Scaled Error; MAE: Mean Absolute Error; RMSE: Root Mean Square Error.

6.3 Convergence calculation of Fitness Augmented African Bison Optimization algorithm

Determining the convergence for the implemented FAABO algorithm in performing the optimal routing differentiated from the existing conventional algorithms for different node variations is defined in Figure 5. The major goal of the designed FAABO is to achieve scalable and reliable routing in the WSN network. It helps in the secure data transmission based on the trusted path selection. Here the number of iterations varied to perform the comparison, which ranges between 0 to 100. From the graphical determination, the initiated FAABO algorithm attained better convergence than 70% of GOA, 35% of YSGA, 32.5% of CWO, and 30% of ABOA. The obtained result defines the better convergence attained by the FAABO algorithm.

6.4 Statistical calculation of the Fitness Augmented African Bison Optimization algorithm

The statistical estimation of the initiated FAABO algorithm differentiated from the other optimization approaches based on different statistical measures is explained in Table 3. Here number of nodes varied to achieve the result to evaluate the effectiveness of the algorithm. The functionality of the FAABO is accessed by the statistical analysis in terms of the optimal path selection in the WSN network. The recommended FAABO attained a better value than 27.7% of GOA, 3.2% of YSGA, 8.7% of CWO, and 6.7% of ABOA. The outcome from the result defines the better functionality achieved by the FAABO than other existing optimization models.

6.5 Performance comparison of HSCRNet-based trust prediction

Performance assessment of the presented HSCRNet model for the trusted node prediction compared with other similar approaches and it expressed in Figure 6. Here, the determination is performed by varying the nodes on different performance measures. This analysis helps in evaluating the performance of HSCRNet in classifying the nodes in the WSN based on the trusted and malicious nodes. From the graphical calculation, the presented HSCRNet attained better accuracy than 4% of Deep Neural Network (DNN), 3% of Long Short-Term Memory (LSTM), 2% of TCN, and 1% of CapsNet. Due to this result, the presented model attained a better result than other approaches.

6.6 Overall comparison of HSCRNet-based trust prediction

The overall comparison of the designed HSCRNet-based trusted node prediction differentiated from the other baseline model expressed in Table 4. Here the number of nodes varied to perform the analysis, along with the different optimizers to evaluate the given models. From the comparison the initiated HSCRNet attained the minimum MEP of 78% of DNN, 59% of LSTM, 35% of TCN, and 12% of CapsNet for the number of nodes 50 while determining with the adam optimizer. Based on the overall comparison the HSCRNet has a better classification result than the other existing approaches.

Each experiment was repeated 20 times using different random seeds. The reported values correspond to mean ± standard deviation.

A paired t-test at a significance level of 0.05 confirmed that the performance improvements achieved by HSCRNet and FAABO were statistically significant compared with baseline methods.

To confirm the effectiveness and efficiency of the HSCRNet-FAABO framework in providing trustworthy and reliable routing solutions for WSNs, all the presented experiments have been conducted 20 times with different random seeds under identical simulation environments. All performance measures have been calculated using mean ± standard deviation (SD). Furthermore, the statistical significance tests, based on a paired t-test at $\alpha = 0.05$, have been used to compare the proposed scheme against the baseline algorithms. As can be seen, all improvements made using HSCRNet and FAABO are statistically significant ($p < 0.05$).

In particular, HSCRNet outperformed DNN (96.94 ± 0.56%, paired t-test = 〈<0.001), LSTM (97.32 ± 0.48%, p-value < 0.001), TCN (97.76 ± 0.41%, p-value = 0.002), and CapsNet (98.21 ± 0.34%, p-value = 0.014) in terms of trusted node classification accuracy. It is noteworthy that, on average, the difference in performance reached 2%, which means that HSCRNet demonstrates superior capabilities in detecting malicious nodes and avoiding security breaches caused by them.

At the same time, FAABO showed better performance compared to GOA (89.71 ± 1.18%, p-value < 0.05), YSGA (91.64 ± 1.04%, p-value <0.05), CWO (93.52 ± 0.88%, p-value < 0.05), and ABOA (95.84 ± 0.73%, p-value <0.05). The average improvements reached 2-5%, demonstrating the superior capabilities of FAABO in providing trustworthy and reliable routing solutions.

Finally, to verify the stability and robustness of the framework, the HSCRNet–FAABO solution was tested in three attack modes: blackhole, wormhole, and sybil attacks. In this experiment, PDR, TCA, and latency have been chosen as performance criteria. Thus, the results for Blackhole attack mode include 96.8 ± 0.42% PDR, 98.2 ± 0.31% trust accuracy, and 0.25 ± 0.01 s delay; for Wormhole attack mode – 95.7 ± 0.47% PDR, 97.8 ± 0.36% trust accuracy, and 0.28 ± 0.02 s delay; and for Sybil attack mode – 94.9 ± 0.53% PDR, 97.3 ± 0.41% trust accuracy, and 0.31 ± 0.02 s delay. A one-way ANOVA test was used to investigate the impact of the type of attacks on the results of the experiments. No statistically significant differences ($P = 0.087$, p-value > 0.05 for trust prediction accuracy and $P = 0.094 > 0.05$) across the considered attack scenarios.

6.7 Comparative analysis of the Fitness Augmented African Bison Optimization algorithm for the optimal routing mechanism

The performance estimation of the presented FAABO algorithm for the optimal route selection in the WSN network compared with the other existing algorithms regarding several nodes and density is defined in Figures 7 and 8. The main aim of this comparative analysis is to determine the routing efficiency based on the secured data transmission. Based on the graphical illustration, the implemented FAABO algorithm achieved the effective result of 80% of GOA, 75% of YSGA, 67% of CWO, and 25% of ABOA for taking the number of nodes as 50. This shows the effectiveness of the algorithm in performing the optimal route selection.

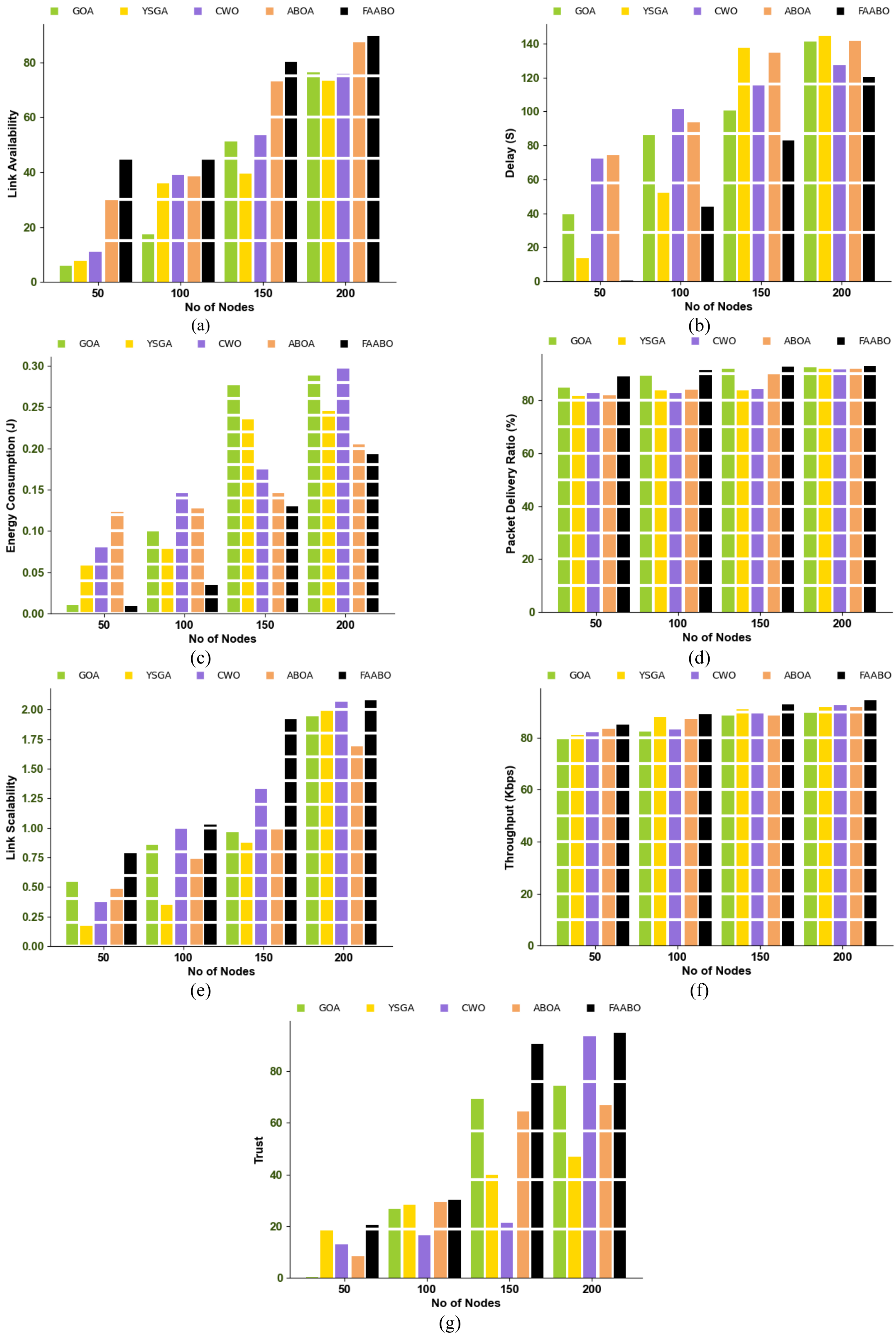


Figure 7. Comparative estimation of the implemented Fitness Augmented African Bison Optimization (FAABO) algorithm in functioning optimal routing compared with other optimization models in terms of "(a) Availability, (b) Delay, (c) Energy consumption, (d) PDR, (e) Scalabiltiy, (f) Throughput, and (g) Trust"

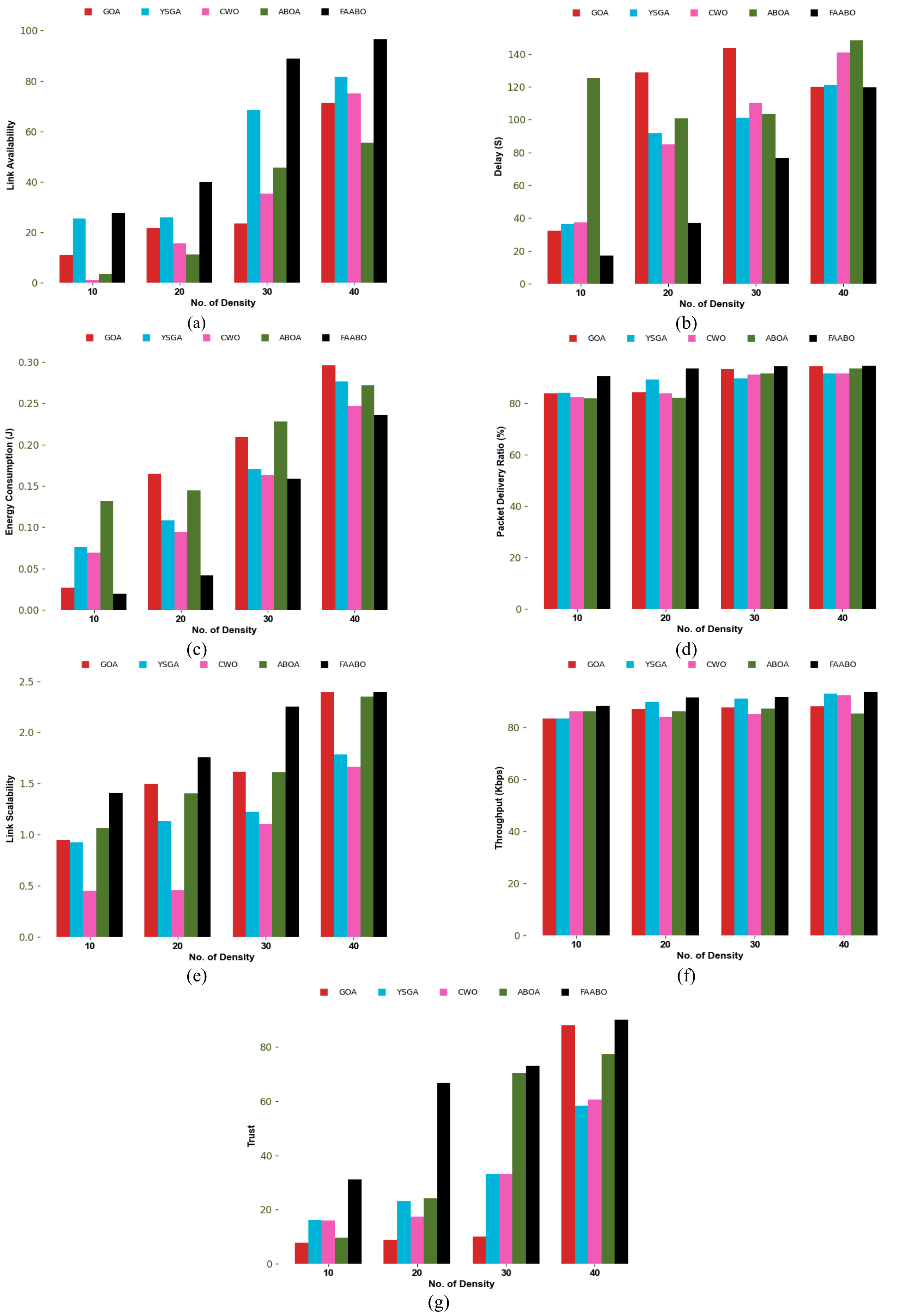


Figure 8. Comparative determination of the suggested FAABO algorithm in performing optimal routing differentiated with other models based on number of density in terms of "(a) Availability, (b) Delay, (c) Energy consumption, (d) PDR, (e) Scalability, (f) Throughput, and (g) Trust"

Table 5. Performance evaluation of the proposed HSCRNet–FAABO framework under different routing attack scenarios

Attack	PDR (%)	Trust Accuracy (%)	Delay
Blackhole	96.8	98.2	0.25
Wormhole	95.7	97.8	0.28
Sybil	94.9	97.3	0.31

Note: PDR: Packet Delivery Ratio; Blackhole: Blackhole Attack; Wormhole: Wormhole Attack; Sybil: Sybil Attack; HSCRNet: Hybrid Serial Cascaded Residual Network; FAABO: Fitness-Augmented African Bison Optimization.

The proposed framework maintained stable routing performance under blackhole, wormhole, and Sybil attack conditions. HSCRNet successfully identified malicious behavior, while FAABO selected alternative trusted paths, preventing severe packet loss in Table 5.

6.8 Computational complexity analysis

The complexity of HSCRNet is O(N×T×F), where N represents the number of nodes, T the temporal sequence length, and F the feature dimension. The routing complexity of FAABO is O(P×I×D), where P denotes population size, I the number of iterations, and D the routing dimension. Although the proposed model introduces additional computation compared with conventional routing protocols, trust prediction is executed periodically at the sink node, minimizing sensor-node overhead.

7. CONCLUSION

This paper presented a trust-aware secure routing framework for WSNs using the HSCRNet and the FAABO algorithm. The proposed HSCRNet model effectively predicts trusted and malicious nodes by exploiting temporal communication characteristics and extracting discriminative features through the integration of TCN and Capsule Network (CapsNet) architectures. Based on the identified trusted nodes, the FAABO algorithm performs multi-objective route optimization to determine secure and energy-efficient communication paths. The performance of the proposed framework was evaluated under different WSN configurations and attack scenarios. Experimental results demonstrated that HSCRNet achieved superior trust prediction accuracy compared with existing methods, while FAABO significantly improved packet delivery ratio, throughput, scalability, trust value, and link availability with reduced delay and energy consumption. The attack-specific evaluation further confirmed the robustness of the framework against blackhole, wormhole, and Sybil attacks by successfully identifying malicious nodes and avoiding compromised routing paths. The proposed HSCRNet–FAABO framework is particularly suitable for medium- and large-scale WSN deployments operating in hostile and resource-constrained environments where secure and trustworthy communication is essential. The integration of deep trust prediction and optimization-based routing provides an effective balance between security, reliability, and energy efficiency. Despite the promising results, the proposed framework has certain limitations. The trust prediction model requires periodic trust updates, and routing performance may be influenced under highly dynamic network topologies with frequent node mobility and rapidly changing communication conditions. In addition, the computational complexity of the optimization process may increase with large-scale network expansion. Future research will focus on developing lightweight adaptive trust-update mechanisms, hybrid optimization strategies, and distributed intelligence-based routing approaches to further enhance scalability, computational efficiency, and secure communication performance in next-generation WSNs.

REFERENCES

[1] Han, Y.J., Hu, H.S., Guo, Y.X. (2022). Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. IEEE Access, 10: 11538-11550. https://doi.org/10.1109/ACCESS.2022.3144015

[2] Haseeb, K., Almustafa, K.M., Jan, Z., Saba, T., Tariq, U. (2020). Secure and energy-aware heuristic routing protocol for wireless sensor network. IEEE Access, 8: 163962-163974. https://doi.org/10.1109/ACCESS.2020.3022285

[3] Prasad, K.H.V., Periyasamy, S. (2023). Secure-energy efficient bio-inspired clustering and deep learning-based routing using blockchain for edge assisted WSN environment. IEEE Access, 11: 145421-145440. https://doi.org/10.1109/ACCESS.2023.3345218

[4] Rhesa, M.J., Revathi, S. (2024). Energy-efficient aware and secure model for WSN lifetime enhancement using HDASCII-AE and GEK-GRU. IEEE Access, 12: 140235-140252. https://doi.org/10.1109/ACCESS.2024.3461794

[5] Suresh, B., Prasad, G.S.C. (2023). An energy efficient secure routing scheme using LEACH protocol in WSN for IoT networks. Measurement: Sensors, 30: 100883. https://doi.org/10.1016/j.measen.2023.100883

[6] Li, C.R., Wu, J.X., Zhang, Z.P., Lv, A.Q. (2023). Energy-harvesting Q-learning secure routing algorithm with authenticated-encryption for WSN. ICT Express, 9(6): 1077-1084. https://doi.org/10.1016/j.icte.2023.05.006

[7] Tabbassum, S., Pathak, R.K. (2024). Effective data transmission through energy-efficient clustering and Fuzzy-Based IDS routing approach in WSNs. Virtual Reality & Intelligent Hardware, 6(1): 1-16. https://doi.org/10.1016/j.vrih.2022.10.002

[8] Vinitha, A., Rukmini, M.S.S., Dhirajsunehra. (2022). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. Journal of King Saud University - Computer and Information Sciences, 34(5): 1857-1868. https://doi.org/10.1016/j.jksuci.2019.11.009

[9] Alotaibi, M. (2021). Improved blowfish algorithm-based secure routing technique in IoT-based WSN. IEEE Access, 9: 159187-159197. https://doi.org/10.1109/ACCESS.2021.3130005

[10] Hu, H.S., Han, Y.J., Yao, M.Q., Song, X. (2022). Trust based secure and energy efficient routing protocol for wireless sensor networks. IEEE Access, 10: 10585-10596. https://doi.org/10.1109/ACCESS.2021.3075959

[11] Anitha, S., Saravanan, S., Chandrasekar, A. (2023). Trust management based multidimensional secure cluster with RSA cryptography algorithm in WSN for secure data transmission. Measurement: Sensors, 29: 100889. https://doi.org/10.1016/j.measen.2023.100889
[12] Onyema, E.M., Suguna, S.K., Sundaravadivazhagan, B., et al. (2025). A secure routing protocol for improving the energy efficiency in wireless sensor network applications for industrial manufacturing. Next Energy, 7: 100219. https://doi.org/10.1016/j.nxener.2024.100219
[13] Fang, W.D., Zhang, W.X., Yang, W., Li, Z.N., Gao, W.W., Yang, Y.X. (2021). Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. Digital Communications and Networks, 7(4): 470-478. https://doi.org/10.1016/j.dcan.2021.03.005
[14] Selvi, M., Thangaramya, K., Ganapathy, S., Kulothungan, K., Nehemiah, H.K., Kannan, A. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. Wireless Personal Communications, 105: 1475-1490. https://doi.org/10.1007/s11277-019-06155-x
[15] Mutalemwa, L.C., Shin, S. (2021). Novel approaches to realize the reliability of location privacy protocols in monitoring wireless networks. IEEE Access, 9: 104820-104836. https://doi.org/10.1109/ACCESS.2021.3099499
[16] Pathak, A., Al-Anbagi, I., Hamilton, H.J. (2022). An adaptive QoS and trust-based lightweight secure routing algorithm for WSNs. IEEE Internet of Things Journal, 9(23): 23826-23840. https://doi.org/10.1109/JIOT.2022.3189832
[17] Qin, D.Y., Yang, S.X., Jia, S., Zhang, Y., Ma, J.Y., Ding, Q. (2017). Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access, 5: 9599-9609. https://doi.org/10.1109/ACCESS.2017.2706973
[18] Bin-Yahya, M., Alhussein, O., Shen, X.M. (2022). Securing software-defined WSNs communication via trust management. IEEE Internet of Things Journal, 9(22): 22230-22245. https://doi.org/10.1109/JIOT.2021.3102578
[19] Xu, M.Y., Zu, Y.X., Zhou, J., Liu, Y., Li, C.Q. (2024). Energy-efficient secure QoS routing algorithm based on elite niche clone evolutionary computing for WSN. IEEE Internet of Things Journal, 11(8): 14395-14415. https://doi.org/10.1109/JIOT.2023.3342091
[20] Yang, L., Lu, Y.Z., Liu, S., Guo, T., Liang, Z.F. (2018). A dynamic behavior monitoring game-based trust evaluation scheme for clustering in wireless sensor networks. IEEE Access, 6: 71404-71412. https://doi.org/10.1109/ACCESS.2018.2879360
[21] Siddiq, A., Ghazwani, Y.J. (2024). Hybrid optimized deep neural network-based intrusion node detection and modified energy efficient centralized clustering routing protocol for wireless sensor network. IEEE Transactions on Consumer Electronics, 70(3): 6303-6313. https://doi.org/10.1109/TCE.2024.3430974
[22] Salim, A., Khedr, A.M., Osamy, W. (2024). Enhancing IoT-enabled sustainable smart cities with secure and energy-aware data collection using meta-heuristic technique. IEEE Sensors Journal, 24(14): 22974-22991. https://doi.org/10.1109/JSEN.2024.3389991
[23] Verma, S., Zeadally, S., Kaur, S., Sharma, A.K. (2022). Intelligent and secure clustering in wireless sensor network (WSN)-based intelligent transportation systems. IEEE Transactions on Intelligent Transportation Systems, 23(8): 13473-13481. https://doi.org/10.1109/TITS.2021.3124730
[24] Ahmed, A., Abdullah, S., Bukhsh, M., Ahmad, I., Mushtaq, Z. (2022). An energy-efficient data aggregation mechanism for IoT secured by blockchain. IEEE Access, 10: 11404-11419. https://doi.org/10.1109/ACCESS.2022.3146295
[25] Feng, W., Wang, F., Xu, D., et al. (2020). Joint energy-saving scheduling and secure routing for critical event reporting in wireless sensor networks. IEEE Access, 8: 53281-53292. https://doi.org/10.1109/ACCESS.2020.2981115
[26] Zhao, J., Wang, K., Wang, J.C., Guo, X.W., Qi, L. (2024). African bison optimization algorithm: A new bio-inspired optimizer with engineering applications. Computers, Materials & Continua, 81(1): 603-623. https://doi.org/10.32604/cmc.2024.050523
[27] Boyle, D., Newe, T. (2008). Securing wireless sensor networks: Security architectures. Journal of Networks, 3(1): 65-77.
[28] Chelli, K. (2015). Security issues in wireless sensor networks: Attacks and countermeasures. In Proceedings of the World Congress on Engineering, London, U.K., pp. 1-6. https://www.iaeng.org/publication/WCE2015/WCE2015_pp519-524.pdf.
[29] Tu, F.F., Liu, D.J., Yan, Z.W., Jin, X.B., Geng, G.G. (2024). STFT-TCAN: A TCN-attention based multivariate time series anomaly detection architecture with time-frequency analysis for cyber-industrial systems. Computers & Security, 144: 103961. https://doi.org/10.1016/j.cose.2024.103961
[30] Bushara, A.R., Kumar, R.S.V., Kumar, S.S. (2024). Classification of benign and malignancy in lung cancer using capsule networks with dynamic routing algorithm on computed tomography images. Journal of Artificial Intelligence and Technology, 4(1): 40-48. https://doi.org/10.37965/jait.2023.0218
[31] Reddy, C.S., Narsimha, G. (2022). Deep neural network with meta-heuristic based trust aware cluster head selection in WSN. Indian Journal of Computer Science and Engineering, 13(4): 1056-1066. https://doi.org/10.21817/indjcse/2022/v13i4/221304042
[32] Du, J.X., Han, G.J., Lin, C., Martínez-García, M. (2022). LTrust: An adaptive trust model based on LSTM for underwater acoustic sensor networks. IEEE Transactions on Wireless Communications, 21(9): 7314-7328. https://doi.org/10.1109/TWC.2022.3157621
[33] Agushaka, J.O., Ezugwu, A.E., Abualigah, L. (2023). Gazelle optimization algorithm: A novel nature-inspired metaheuristic optimizer. Neural Computing and Applications, 35: 4099-4131. https://doi.org/10.1007/s00521-022-07854-6
[34] Zaldívar, D., Morales, B., Rodríguez, A., Valdivia-G, A., Cuevas, E., Pérez-Cisneros, M. (2018). A novel bio-inspired optimization model based on yellow saddle goatfish behavior. Biosystems, 174: 1-21. https://doi.org/10.1016/j.biosystems.2018.09.007
[35] Alomari, S., Kaabneh, K., AbuFalahah, I., et al. (2024). Carpet weaver optimization: A novel simple and effective human-inspired metaheuristic algorithm.

International Journal of Intelligent Engineering & Systems, 17(4): 230-242. https://doi.org/10.22266/ijies2024.0831.18