I.J. Information Technology and Computer Science, **2026, 4, 68-84**
Published Online on August 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2026.04.05

An Improved Trust-based and Energy Efficient Secure Routing Protocol for 5G-WSN

Sachin B. M.*
School of Electronics and Communication Engineering, REVA University, Bengaluru-560064, Karnataka, India
ECE Department, Bangalore Institute of Technology, V V Pura, K R Road, Bengaluru-560004, Karnataka, India
E-mail: sachinbm99@gmail.com
ORCID iD: https://orcid.org/0009-0003-6696-5139
*Corresponding author

Mrinal Sarvagya
School of Electronics and Communication Engineering, REVA University, Bengaluru-560064, Karnataka, India
E-mail: mrinalsarvagya@reva.edu.in
ORCID iD: https://orcid.org/0000-0002-3552-3210

Received: February 10, 2026; Revised: April 10, 2026; Accepted: May 27, 2026; Published: August 8, 2026

Abstract: The 5G-enabled Wireless Sensor Networks (WSNs) leverage the enhanced capabilities of 5G technology to evolve conventional WSN environments. WSN performance may be affected by interference from high-density 5G networks. The novel Hummingbird-based Graph Bernoulli Binomial Trust Management Network (HBbGBBTMN) proposed in this research aims to enhance smart, secure, and energy-efficient routing in 5G-enabled wireless networks. Python is initially used to simulate and model the network under consideration, accounting for fluctuating network conditions and dynamic node behaviors. An improved Hummingbird algorithm is used to detect and remove nodes with high energy consumption, thereby minimizing routing inefficiencies and avoiding suspicious behavior. To protect data integrity and prevent route disruption, malicious nodes are continuously detected and removed. The trust of the remaining nodes is calculated using the Bernoulli-Binomial distribution, which estimates each node's trust based on its previous packet-forwarding history. Such trust mechanisms are combined with node energy levels as well as network dynamics to form a fitness function that identifies optimal routing patterns. The proposed system is validated through extensive performance analysis, including measurements of packet delivery ratio, throughput, packet drop rate, delay, and malicious node prediction accuracy. The findings indicate that in decentralized wireless environments, HBbGBBTMN significantly enhances network efficiency, security, and dependability.

Index Terms: Wireless Network System, Malicious Node, Secure Routing Path, Bernoulli-Binomial Probability Distribution, Prediction.

1. Introduction

Due to their scalability and capacity to monitor and transmit vital data in real time, Wireless Sensor Networks (WSNs) have become an essential part of contemporary communication systems [1]. Because WSNs offer decentralized, affordable, and dependable data collecting and communication, they are extensively utilized in a wide range of applications [2], including smart cities, industrial automation, healthcare, and environmental monitoring [3]. Significant benefits, such as increased bandwidth, ultra-low latency [4], massive device connectivity [5, 6], and support for extensive Internet of Things (IoT) deployments [7], are provided by combining 5G technology with WSNs. These characteristics enable new applications requiring dependable [8], fast, and low-latency data exchange, such as smart energy management [9], real-time surveillance, and autonomous vehicles [10]. Although 5G offers many benefits, there are several obstacles to overcome before it can be implemented in WSNs [11]. 5G-enabled WSNs operate in dense network environments, which can cause interference, network congestion [12], and reduced quality of service. Furthermore, energy-efficient communication is a crucial requirement, as sensor nodes are frequently resource-constrained, with limited battery power [13], processing capability, and storage [14]. The presence of malicious or misbehaving nodes introduces security risks such as data manipulation [15], packet loss, and denial-of-service attacks [16], jeopardizing the reliability and integrity of transmitted information and complicating network operations [17]. These coupled criteria necessitate the development of routing protocols that effectively control energy consumption,

provide secure communication [18], and uphold high network dependability [19].

In WSNs, routing protocols are responsible for determining the optimal paths for data packets to travel from source nodes to sink nodes [20]. Conventional routing techniques often focus on security or energy efficiency [21], but they rarely combine the two into a cohesive framework suitable for high-density 5G networks [22]. Certain protocols have used trust-based procedures to assess nodes' dependability based on past behavior, thereby lessening the impact of malicious activity [23]. These techniques, however, often ignore energy expenditure, leading to suboptimal routing and a shorter network lifetime [24]. Similarly, energy-aware protocols prioritize battery preservation but may overlook security risks, leaving the network vulnerable to intrusions [25]. As a result, in heterogeneous 5G-enabled WSN systems, there is a glaring gap in the design of routing protocols that simultaneously account for energy efficiency, trustworthiness, and secure data delivery. This study proposes the Hummingbird-based Graph Bernoulli-Binomial Trust Management Network (HBbGBBTMN) as a solution to these issues. To guarantee safe and effective data transfer, the proposed protocol combines energy-aware routing with a trust assessment system. By identifying and eliminating nodes that exhibit malicious activity or high energy consumption, the enhanced Hummingbird algorithm minimizes routing inefficiencies and averts possible security breaches. The Bernoulli-Binomial probability distribution, which assesses each node's dependability based on past packet-forwarding behavior, is used to compute trust levels. A fitness function that guides optimal routing decisions is created by combining these trust scores with energy measures and network dynamics.

In-depth Python simulations are used to assess HBbGBBTMN's performance in dynamic network scenarios. Compared with current routing techniques, the proposed protocol significantly improves network efficiency, reliability, and security, as evidenced by key performance metrics such as packet delivery ratio, throughput, delay, packet drop rate, and malicious node detection accuracy. According to the findings, HBbGBBTMN offers a potential foundation for enabling safe, reliable, and energy-efficient communication in next-generation 5G-enabled WSNs, addressing key issues in contemporary wireless networks.

The critical contributions of this work are presented as follows:

- Initially, a 5G-enabled wireless network is modeled and simulated using Python to emulate dynamic node behavior and network conditions.
- Secondly, an innovative Hummingbird-based Graph Bernoulli Binomial Trust Management Network (HBbGBBTMN) is introduced to enable intelligent, secure, and energy-efficient routing.
- An improved Hummingbird fitness function is employed to detect and eliminate high-energy-consuming nodes, reducing overload and routing inefficiencies and avoiding suspicious node behaviour.
- Malicious suspected nodes are dynamically detected and isolated to minimize the risk of route disruption.
- The remaining nodes are assessed for trustworthiness using the Bernoulli-Binomial distribution, which evaluates each node’s historical forwarding behaviour to compute trust levels.
- The routing path is optimized using a fitness function that balances trust values, energy status, and network dynamics, ensuring the selection of secure, efficient routes.
- Subsequently, the designed network performance is validated regarding packet delivery, throughput, packet drop, malicious prediction, and delay.

Section 2 reviews related works, and Section 3 outlines the problem statement. Section 4 details the proposed methodology, Section 5 presents the performance evaluation, and Section 6 concludes the work.

2. Related Works

The following is a summary of several research works currently associated with this study:

Due to energy limitations, WSNs face challenges that affect their efficiency and lifespan. For that reason, Gururaj et al. [26] proposed a collaborative energy-efficient routing protocol (CEEPR) to support sustainable communication in 5G/6G WSNs. The protocol supports performance improvement through the deployment of a multi-objective improved seagull algorithm (MOISA), cluster head selection based on residual energy, and reinforcement learning. Additionally, the suggested strategy reduces energy usage by 50% while also enhancing the network's durability and efficiency. However, while it performs well in cluster head selection, its implementation relies on limited resources, which may restrict scalability.

Wakili et al. [27] introduced a machine learning-aided solution to improve the Routing Protocol for Low-Power and Lossy Networks (RPL) for IoT networks. The architecture involves a random forest classifier for traffic type detection, an enhanced RPL objective function, and a reinforcement-learning module for dynamic routing control. The augmented framework improves jitter, increases the packet delivery ratio (PDR), reduces delay, and provides better end-to-end throughput, as shown in simulation results. This paper explains the end-to-end solution for improving the RPL mechanism and protecting against standard security attacks. Nevertheless, it incurs high computational overhead.

Shanmathi et al. [28] applied fuzzy logic and a convolutional neural network to examine the extent to which WSNs are vulnerable to malicious attacks. The method efficiently separates malicious nodes from trustworthy ones, and an enhanced routing technique that utilizes a Neuro Genetic Optimizer improves WSN lifetime, reduces latency, and

outperforms current protocols in terms of energy efficiency and packet delivery ratio. However, in some cases, it affects the malicious prediction rate.

WSNs are subject to different types of network attacks. Li et al. [29] use enhanced Q-learning and physical unclonable functions to ensure the integrity of the transmission line. Additionally, the residual energy of nodes is predicted using an LSTM-based model. Through simulations, the suggested algorithm's effectiveness is contrasted with that of alternative methods under various attacks. The proposed method improves PDR, reduces node energy consumption, and enhances selfish node filtering. However, in some rare cases, it faces security overhead that consumes more energy and power.

Sharma et al. [30] present a hybrid routing technique for Energy-Efficient IoT WSN applications with reduced energy consumption. In order to better route, it integrates an energy-aware heuristic mechanism with swarm optimization. Particle Swarm Optimized Residual Energy-Based Stable Election Protocol reduces the cycle of cluster head selection and achieves scalability in the network. The method improves on earlier heterogeneous algorithms in terms of energy consumption, alive nodes, and network lifetime. However, it may result in unreliable communication paths, leading to increased packet loss during transmission.

3. Problem Statement

Significant issues arise in energy management, routing effectiveness, and security when 5G is integrated with WSNs. Due to the inability of traditional routing methods in WSNs to identify and isolate rogue nodes, data integrity is compromised, energy consumption is uneven, network congestion occurs, and network lifetime is shortened. Additionally, current methods do not combine energy-aware routing with trust-based processes, leading to ineffective communication and increased susceptibility to attacks. An intelligent routing system that can detect hostile nodes, maximize energy use, guarantee dependable data transfer, and improve overall network security is therefore urgently needed. The Hummingbird-based Graph Bernoulli-Binomial Trust Management Network (HBbGBBTMN), which combines node trust assessment with energy-aware routing to identify and isolate malicious nodes, increase network efficiency, and lengthen network lifetime, is proposed in this article as a solution to these problems. Fig. 1 illustrates the system model highlighting these challenges.

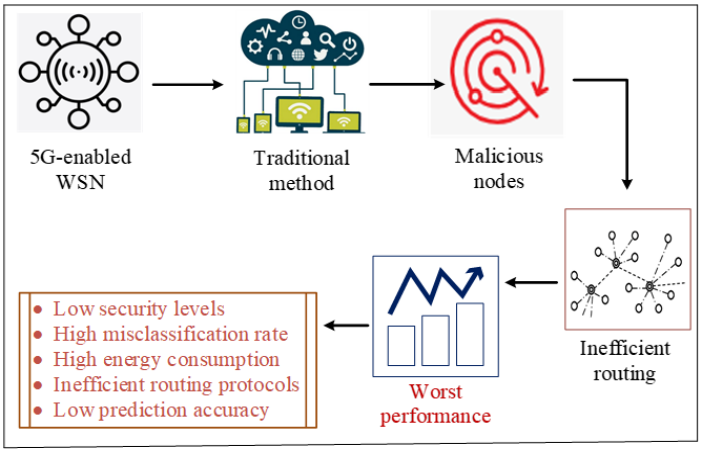

Fig.1. System model illustrating network challenges

4. Proposed Methodology

An innovative Hummingbird-based graph Bernoulli Binomial trust management network (HBbGBBTMN) has been introduced to enable intelligent, secure, and energy-efficient routing. Initially, a 5G-enabled wireless network is modeled and simulated using Python to simulate dynamic node behaviour and network conditions. An improved Hummingbird fitness function is employed to detect and eliminate high-energy-consuming nodes, reducing overload and routing inefficiencies and avoiding suspicious node behaviour. Malicious suspected nodes are dynamically detected and isolated to minimize the risk of route disruption. The remaining nodes are assessed for trustworthiness using the Bernoulli-Binomial distribution, which evaluates each node's historical forwarding behaviour to compute trust levels. The routing path is optimized using a fitness function that balances trust values, energy status, and network dynamics, ensuring the selection of secure, efficient routes. Subsequently, the designed network performance is validated regarding packet delivery, throughput, packet drop, malicious prediction, and delay. The proposed architecture is illustrated in Fig. 2.

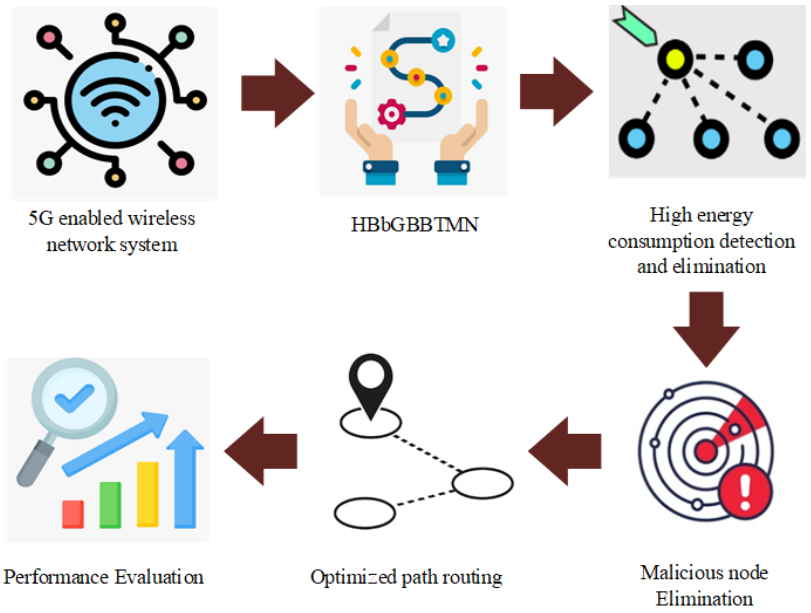

Fig.2. Proposed architecture

4.1. Process of the proposed HBbGBBTMN

This paper introduces the Hummingbird-based graph Bernoulli Binomial trust management network to enable intelligent, secure, and energy-efficient routing. The various phases of the new HBbGBBTMN were discussed, including network design, high-energy consumption prediction, malicious node detection, and secure routing path selection.

A. Network Design

In the first stage, the 5G wireless network is modeled and simulated on the Python platform. Based on simulations of node parameters such as mobility, energy consumption, and communication protocols, the environment emulates the dynamic aspects of wireless communication. The network design can be represented in Eqn. (1).

$$W_o = \{N_1, N_2, N_3, \ldots\ldots, N_m\} \tag{1}$$

Here, W_o represents the network design variable, and N denotes the nodes, $N_1, N_2, N_3, \ldots\ldots, N_m$ is the m number of nodes in the designed network.

B. High-energy Consumption Node Prediction

Subsequently, high-energy-consuming nodes are identified and removed using an improved Hummingbird-inspired fitness function to improve energy efficiency and prolong the network's operational lifetime. These nodes typically exhibit a significant decrease in residual energy due to malicious activity, excessive data transmission, or reception overhead. The energy consumption rate of each node is continually monitored over time by the specification in order to identify these nodes systematically. The prediction of high energy consumption is formulated in Eqn. (2).

$$CE_j = \frac{L_{j,initial} - L_{j,current}}{\nabla y} Tb \tag{2}$$

Here, $L_{j,initial}$ denotes the initial energy of node j, $L_{j,current}$ signifies the energy that remains in node j, ∇y indicates the quantity of cycles of communication, Tb denotes the hummingbird fitness function and CE_j is the high energy consumption node prediction parameter. When a node $CE_j > X$ is removed from routing pathways because of its high energy consumption, where $(X = \theta)$. The enhanced Hummingbird optimization technique removes such nodes from the routing pool in order to minimize network overload, increase network lifespan, and improve total routing performance here, X is the threshold range parameter.

C. Malicious Node Detection

In a 5G-enabled WSN, identifying and removing rogue nodes is necessary for effective, secure communication. The packet-forwarding behavior of each node is continuously observed. If a node regularly misses packets, alters data, or neglects to forward messages, it is deemed suspect. Such actions could be a sign of malicious activity, which could lead to network failures or route disruptions. To identify malicious nodes, for each node i, the score of the malicious characteristics z_i is computed by Eqn. (3), here, Q_i is the packets that forwarded successfully, and is the number of

packets failed during the forwarding processF_i. The more suspicious behavior is denoted as $z_i \in [0,1]$

$$z_i = \frac{F_i}{Q_i + F_i} \tag{3}$$

$$H_s^i = \begin{cases} Normal & z_i \leq \theta \\ Malicious & z_i > \theta \end{cases} \tag{4}$$

Here, H_s^i denotes the node status in Eqn. (4), θ is the Malicious behavior threshold (typical value: 0.5, adjustable based on network requirements). Nodes with z_i beyond the threshold are regarded as malicious and are not taken into account when making routing decisions, preventing route disruption and safeguarding data integrity.

The Bernoulli-Binomial trust model is used to assess the reliability of surviving nodes after malicious nodes are isolated. Packet forwarding is treated as a binary outcome—success or failure—in this statistical method. A node's consistent contribution to network functionality is indicated by a higher trust rating, which also aids in selecting reliable, energy-efficient routing paths.

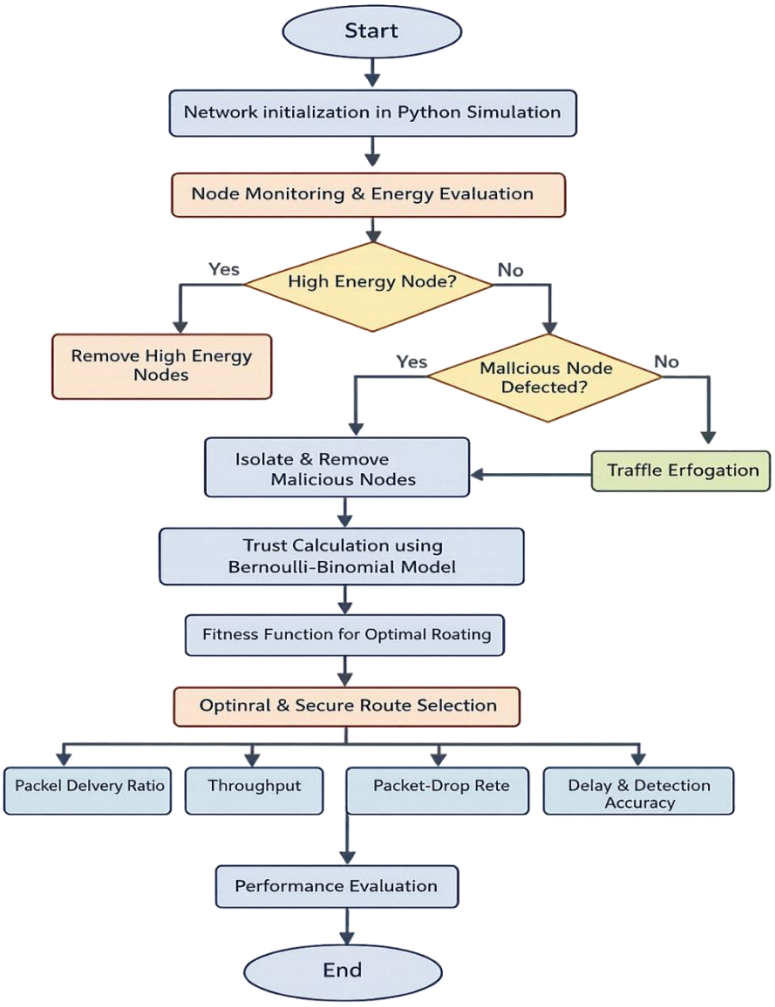

Fig.3. Flowchart of HBbGBBTMN

D. Optimizing Secure Routing Path

Following the detection and isolation of malicious nodes, the remaining nodes are assessed for network dynamics, energy efficiency, and trustworthiness. The proposed Hummingbird fitness model accounts for potential route impediments, such as malicious nodes. During the optimization process, nodes with sufficient energy are selected to form new paths. Upon detection of malicious nodes, the routing protocol dynamically adjusts to establish alternative secure routes. To improve data transfer and reduce transmission delays, a new path has been developed. A trusted node is a normal node that remains after predicted malicious nodes are identified and eliminated. It ensures that the data transmission path is the most stable, energy-efficient, and secure. The optimized secure routing path is illustrated in Eqn. (5).

$$G_{route} = \sum_{j\in path}^{\Sigma}(\lambda.R_j + \eta.\frac{F_j}{F_{max\,j}} \quad (5)$$

Where G_{route} signifies the overall fitness score of a routing path, R_j denotes the node's trust value, F_j represents the residual energy of node j, F_{max} is the maximum energy, and λ, η, ϑ are the weight factors and D_j is the shortest path. These weight coefficients indicate the importance of the factors included in the routing selection process. The routing algorithm selects the path with the highest fitness score after evaluating each feasible route. Thus, the 5G wireless network has a highly robust, adaptable routing system that enhances reliability and performance. The algorithm for the present work is described in Algorithm 1.

Algorithm 1 details the methods and processes of the proposed framework. In a 5G-capable wireless sensor network, the HBbGBBTMN method initializes node energy and trust values. At each iteration, the Hummingbird-based optimization algorithm identifies nodes with excessive energy consumption, which are then excluded from routing. Malicious nodes are identified and separated, and trust levels are updated based on packet forwarding behavior. A fitness function based on trust, energy, and latency is used to construct and assess multiple routing paths. Network parameters are dynamically updated, and the most secure path for data transmission is chosen.

Algorithm 1: HBbGBBTMN

```
Initialize network with all sensor nodes
Assign initial energy value to each node
Assign initial trust value to each node
Set malicious node list as empty
For each iteration do
    // Hummingbird Energy Optimization Phase
    For each node in network do
        Measure current energy consumption
        If energy consumption is high then
            Mark node as inefficient
        End If
    End For
    Remove inefficient nodes from network
    // Trust Evaluation Phase
    For each remaining node do
        Observe packet forwarding behavior
        Update success and failure counters
        Compute trust value
        If trust value is below threshold then
            Mark node as malicious
        End If
    End For
    Add malicious nodes to malicious list
    Remove malicious nodes from network
    // Hummingbird Routing Search Phase
    Generate multiple candidate routing paths
    For each path do
        Evaluate path based on:
            - Average trust of nodes
            - Average remaining energy
            - Total transmission delay
    End For
    Select best path with highest fitness
    // Data Transmission Phase
    Transmit data using selected path
    Update node energy levels
    Update trust values
End For
Return best routing path and malicious node list
```

5. Result and Discussion

To demonstrate the effectiveness of the proposed model, performance is evaluated using several metrics. The performance of the proposed HBbGBBTMN is evaluated with varying numbers of nodes (N=20 to 100). A comparison of specific parameters with existing methods illustrates the efficacy of the concept. Table 1 describes the parameter execution.

Table 1. Execution parameter

Parameter	Description
Operating system	Windows 10
Platform	Python
Version	3.7.14
Network type	WSN
Number of nodes	100
Optimization	Humming bird

Python (version 3.7.14) was used to implement and evaluate the proposed HBbGBBTMN protocol on a Windows 10 system. A two-dimensional deployment area was used to mimic a wireless sensor network environment with 100 sensor nodes. Throughout the simulation, nodes remained stationary and were randomly dispersed.

To simulate actual wireless communication, a log-distance path loss radio model was used. Every node has a defined broadcast range and an omnidirectional antenna. Sensor nodes periodically sent sensed data toward the sink node, and data transmission followed a constant bit rate traffic model. The packet size was fixed at 512 bytes. To ensure statistical fairness and repeatability, the simulation was run for 1000 communication rounds, and the outcomes were averaged across multiple independent runs with different random seeds. To ensure uniformity across all compared methods, a fixed random seed was utilized for every run. Energy was used during transmission, reception, and idle states in an energy model based on the first-order radio energy consumption model. Every node started with the same amount of energy, and energy loss was continuously monitored throughout the simulation. An attacker model, in which a portion of nodes acted maliciously by deliberately deleting or misrouting packets, was proposed in order to assess security performance. Between 10% and 30% of the network was composed of malicious nodes. By discarding forwarded packets and fraudulently advertising routes, these hostile nodes sought to interfere with routing. During route creation, reliable and energy-efficient nodes were dynamically chosen using the Hummingbird optimization technique. To ensure a fair comparison, all protocols were evaluated under the same network configurations, traffic patterns, and attacker setups.

5.1. Case Study

The purpose of this case study is to offer the optimal path of the proposed HBbGBBTMN. First, the necessary number of 100 source nodes was determined. A Python program generates the nodes, which are then placed randomly in the network. The hummingbird fitness was embedded in the suggested method.

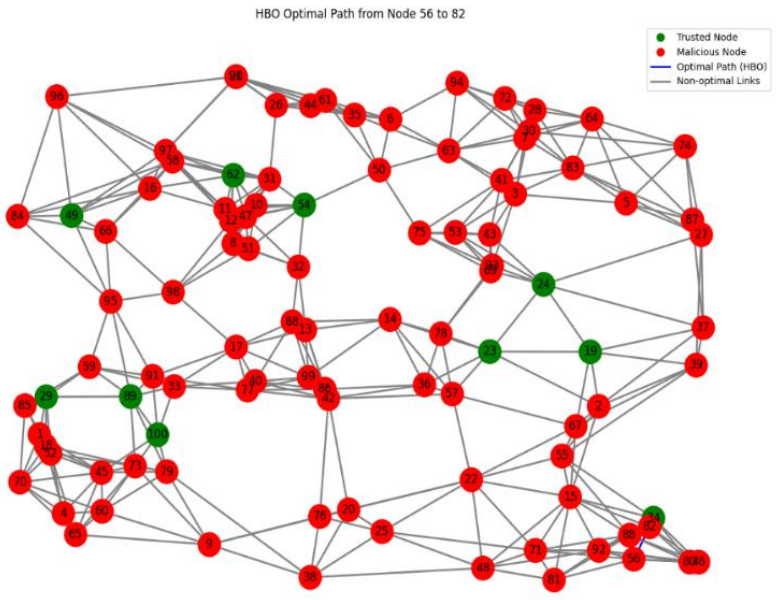

Fig.4. Routing path

A network graph with nodes classified as malicious or trusted is shown in Fig. 4. The goal is to use the Hummingbird Optimization (HBO) method to determine the optimal route from Node 56 to Node 82. The gray edges show other inefficient connections within the network. The HBO algorithm effectively locates secure routes through trusted nodes, ensuring that data is transmitted on a more secure path while avoiding dangers, even in the occurrence of a high frequency of hostile nodes.

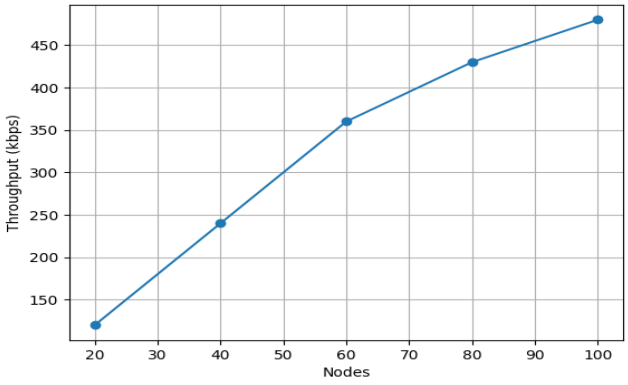

Fig.5. Throughput graph

The throughput graph (Fig. 5) shows how the number of sensor nodes and the network's achieved data throughput are related. The throughput steadily improves as the number of nodes rises from 20 to 100. This behavior shows that, even with a higher node density, the suggested HBbGBBTMN protocol effectively utilizes the network resources at its disposal and establishes reliable routing paths. By choosing reliable, energy-conscious routes, the Hummingbird-based optimization mechanism reduces packet loss and retransmissions, boosting overall data delivery performance. The growing trend validates that the suggested routing solution is scalable for dense 5G-enabled WSN environments.Fig. 6 shows the packet drop graph.

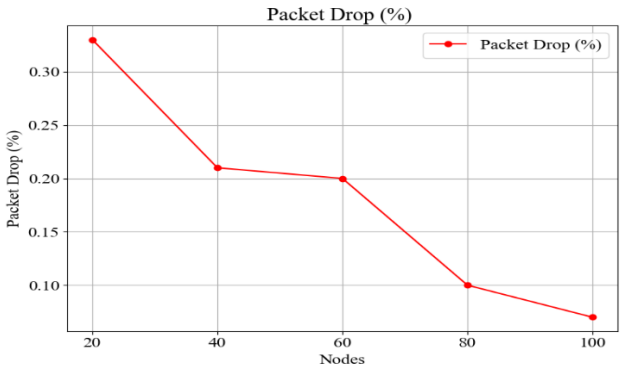

Fig.6. Packet drop graph

Packet drop is plotted against node size in this plot, which clearly shows a reduction in packet loss as the network grows from 20 to 100 nodes. The packet drop rate is around 0.32% at 20 nodes, but it drops to below 0.07% at 100 nodes. This downward trend indicates that the routing protocol can better find reliable, stable paths as the network becomes denser, with less disruption by malicious nodes or network failures. Improved data transport and greater dependability are provided by larger networks' greater redundancy and provision of backup routes.

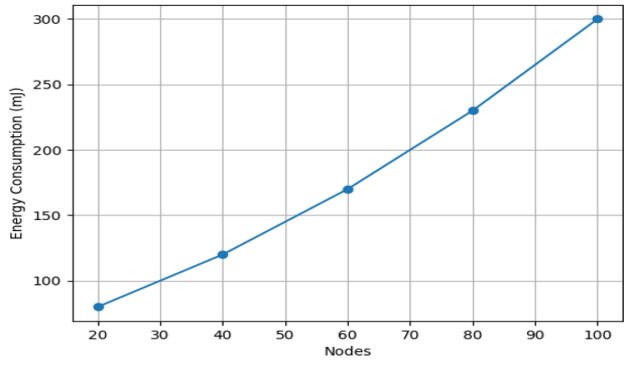

Fig.7. Energy consumption graph

The network's overall energy consumption relative to the number of sensor nodes is displayed in the energy consumption graph (Fig. 7). As would be predicted, as network size increases, so does overall energy use. This is because more nodes result in more communication activity, including greater routing overhead, packet transmissions, and receptions. However, by removing malicious and inefficient nodes and choosing energy-efficient routing methods, the suggested HBbGBBTMN protocol maintains regulated energy growth despite the upward trend. This indicates that the protocol strikes a reasonable compromise between energy efficiency and performance, which is essential for wireless sensor networks to function over the long term.

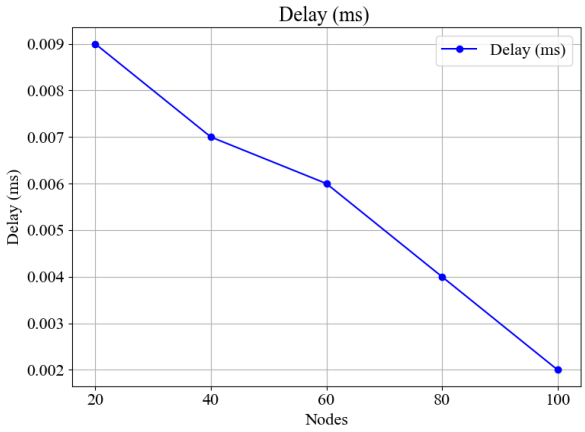

Fig.8. Delay graph

The network delay is plotted against the number of nodes in Fig. 8, clearly showing that the delay decreases with network growth. The delay is around 0.009 ms at 20 nodes and then decreases to about 0.002 ms at 100 nodes. This pattern suggests that larger networks can more effectively select fewer or faster channels, avoid overloaded or malicious nodes, and increase overall communication speed—all made possible by improved routing techniques such as the HBO methodology. The delay reduction directly supports applications that require low delay performance in rapidly evolving networks.

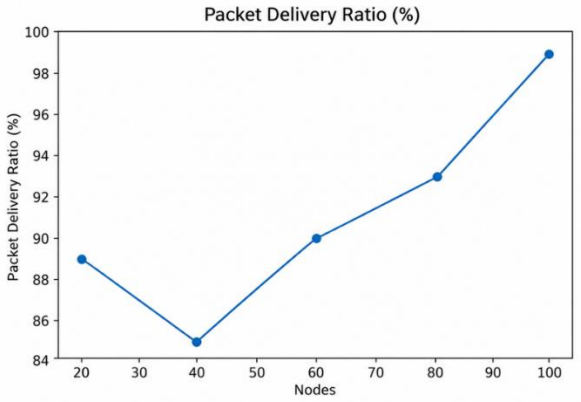

Fig.9. PDR graph

Fig. 9 displays the packet delivery ratio as a percentage as a function of the number of nodes in the network. At 20 nodes, the PDR is high; however, at 40 nodes, it decreases significantly, likely due to initial network congestion. Nevertheless, the PDR gradually improves as the total number of nodes increases, reaching about 99% at 100 nodes. This rising pattern suggests that as node density increases, the network becomes more reliable and efficient. This is certainly because improved connection and route redundancy lead to enhanced successful packet transmissions.

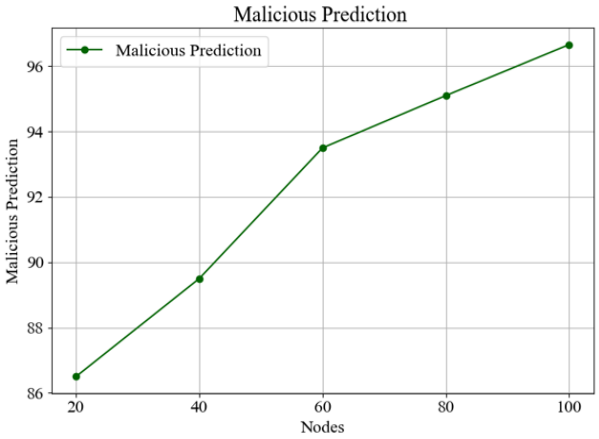

Fig.10. Malicious prediction graph

Fig.10 illustrates the rate of malicious predictions for a series of network node numbers. The prediction rate for malicious nodes increases from approximately 86% to approximately 97% as the number of nodes increases from 20 to 100. This pattern suggests that the larger the network, the more effective the detection model at identifying malicious behavior. The improved ability of the prediction system to distinguish between trustworthy and malicious nodes may be due to the greater amount of data that is available for evaluation. Fig. 11 shows the confusion matrix.

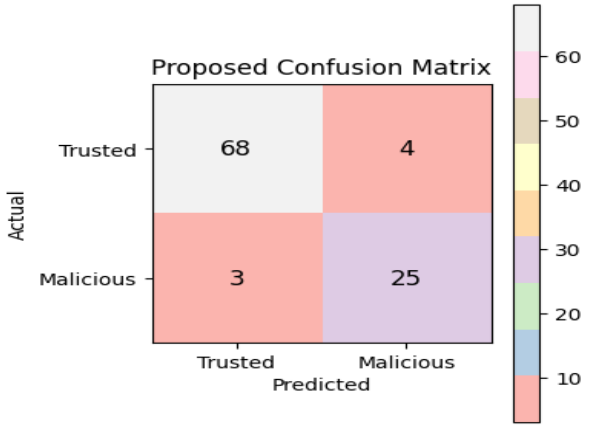

Fig.11. Confusion matrix

The confusion matrix in Fig. 11 shows how well the suggested HBbGBBTMN trust-based classification system distinguishes between malicious and trusted sensor nodes. A network of 100 nodes is used for the evaluation. Four trusted nodes are mistakenly identified as malicious, whereas 68 of the total trusted nodes are correctly classified as trusted. Legitimate nodes are rarely misclassified, as seen by the extremely low false alert rate. In a similar vein, only 3 harmful nodes are mistakenly categorized as trusted, whereas 25 malicious nodes are clearly identified as such. This indicates that the suggested approach has strong detection capabilities and successfully identifies damaging or aberrant network behavior. The suggested HBbGBBTMN procedure achieves high classification accuracy with few misclassifications, as confirmed by the overall confusion matrix. The outcomes confirm the dependability of using Hummingbird optimization in conjunction with Bernoulli-based trust evaluation for secure routing in 5G-enabled wireless sensor networks.

5.2. Performance Analysis

The efficacy of the proposed model is evaluated using metrics including energy consumption, malicious prediction accuracy, throughput, latency, and packet loss rate. To ensure its performance increase, it is compared with a few existing techniques such as Energy Aware on Demand Routing Protocol (EA-DRP), Energy Efficient Optimized hierarchical Routing Algorithm (EE-OHRA), Bacterial Foraging Optimization Algorithm (BFOA) [31], Distributed Congestion Control Protocol (DCCP), Packet Priority Intimation-based Congestion Control Mechanism (PPI), Intelligent Video Surveillance Platform (IVSP), and NoDPCC [32].

All baseline routing methods (EA-DRP, EE-OHRA, and BFOA) as well as the suggested HBbGBBTMN approach were implemented and assessed using the same network setups, simulation times, traffic patterns, and energy models to ensure an equitable and repeatable comparison. The wireless sensor network consisted of 100 randomly placed nodes in a 1000 x 1000 m area. Each node had a transmission range of 100 m, static locations, and an initial energy of 1 joule. Over the course of 1000 simulation rounds, traffic used a Constant Bit Rate model with 512-byte packets. To guarantee

constant computational budgets for optimization-based techniques (BFOA and HBbGBBTMN), the population size was set to 30 agents and the maximum number of iterations to 100. The EA-DRP parameters were configured as follows: route discovery interval = 5 s, neighbor update interval = 2 s, energy threshold = 30% of initial energy, maximum hops = 10, route maintenance timeout = 10 s, and forwarding probability = 0.8. The EE-OHRA parameters were set as follows: opportunistic window = 3 s, energy threshold = 25%, link quality threshold = 0.6, route refresh interval = 6 s, forwarding probability = 0.75, and candidate forwarders = the top 5 neighbors. The BFOA parameters were established as follows: population size = 30 bacteria, chemotactic steps = 20, reproduction steps = 10, elimination-dispersal events = 5, step size = 0.1, and maximum iterations = 100. Additionally, trust update and node elimination mechanisms were integrated into the proposed HBbGBBTMN at each iteration with negligible computational overhead. Using the same framework, all metrics—throughput, energy consumption, delay, and malicious node prediction accuracy—were averaged across 10 simulation runs with different random seeds. To ensure fair and reproducible comparisons, these parameter values, which align with standard configurations in WSN and swarm-based routing literature, were consistently applied.

A. Packet Delivery Ratio

Packet Delivery Ratio (PDR), a key metric in wireless networks, particularly WSNs, measures the ratio of successfully received packets to the total number of transmitted packets. The PDR is calculated using Eq. (6).

$$PDR = \frac{Totalreceivedpackets}{Totalsentpackets} \tag{6}$$

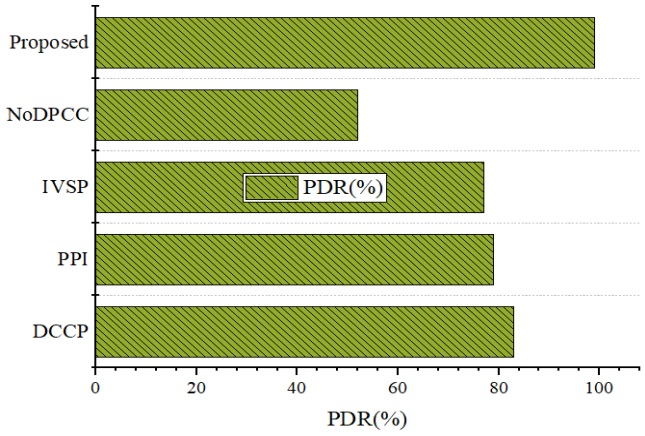

Fig.12. Comparison of PDR

As shown in Fig. 12, the proposed HBbGBBTMN method exhibits more stable PDR values compared to the DCCP, PPI, IVSP, and NoDPCC protocols. The PDR achieved by HBbGBBTMN is higher than that of existing methods. Conversely, the maximum PDR values of other protocols remain lower. Table 2 presents the packet delivery ratios of existing methods.

Table 2. Packet Delivery Ratio of Existing Methods

Methods	Percentage (%)
DCCP	83
PPI	79
IVSP	77
NoDPCC	52
Proposed	99

B. Throughput

Throughput is a critical metric in wireless networks that quantifies the rate of successful data transmission from source to destination. Throughput is calculated using Eq. (7).

$$Throughput = \frac{Totalno.ofreceiveddata}{Totalno.oftransmissiontime} \tag{7}$$

Higher throughput indicates better system performance. The throughput metrics for the HBbGBBTMN simulations are presented below. Fig. 13 shows the comparison of throughput.

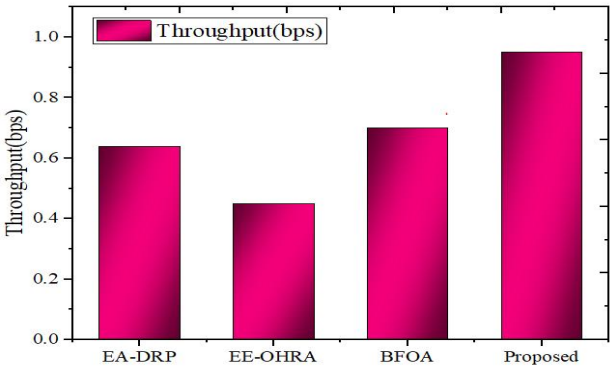

Fig.13. Comparison of Throughput

C. Energy Consumption

Energy consumption refers to the total energy expended by sensor nodes for sensing, processing, transmission, and reception. Energy consumption is calculated using Eq. (8).

$$Energyconsumption = T_e + R_e + I_e \tag{8}$$

Here, T_e represents the transmitted energy, R_e represents the received energy, and I_e denotes the idle energy.

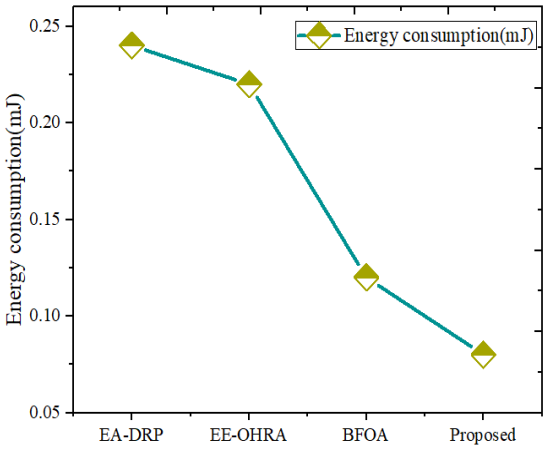

Fig.14. Comparison of Energy Consumption

Fig. 14 shows the comparison of energy consumption. In comparison, the EA-DRP protocol consumed 0.24 mJ, the BFOA method consumed 0.12 mJ, and the EE-OHRA technique consumed 0.22 mJ. In contrast, the proposed approach consumed only 0.08 mJ.

D. Delay

Delay in WSN refers to the time required for a data packet to be transmitted from its source to its destination. This delay is a critical performance metric that affects data transfer efficiency and the overall network performance. The delay can be illustrated as Eqn. (9).

$$Averagedelay = Pa_t - Ps_t \tag{9}$$

Here, Ps_t denotes the packet sending time, and Pa_t denotes the packet receiving time.

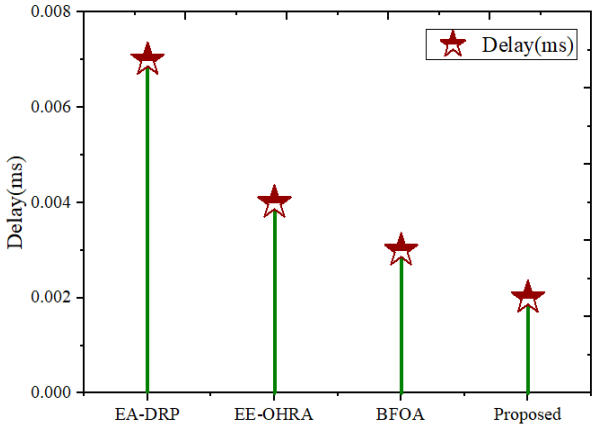

Fig.15. Comparison of Delay

Fig. 15 shows the comparison of delay. The proposed HBbGBBTMN method achieves the lowest delay of 0.002 ms, whereas the EA-DRP protocol exhibits the highest delay among the compared protocols.

E. Malicious Prediction Accuracy

A system's capacity to accurately detect nodes demonstrating malicious or incorrect activity is termed malicious node prediction. This metric is essential to ensure network security and stability in the context of HBbGBBTMN. The accuracy of malicious predictions can be calculated using Eq. (10).

$$Malicious\,\Pr ediction\ accuracy = \frac{HB_p + HB_n}{HB_p + KL_p + HB_n + KL_n} \tag{10}$$

Here, HB_p is the true positive HB_n signifies the true negative, KL_p denotes the false positive, and KL_n denotes the false negative.

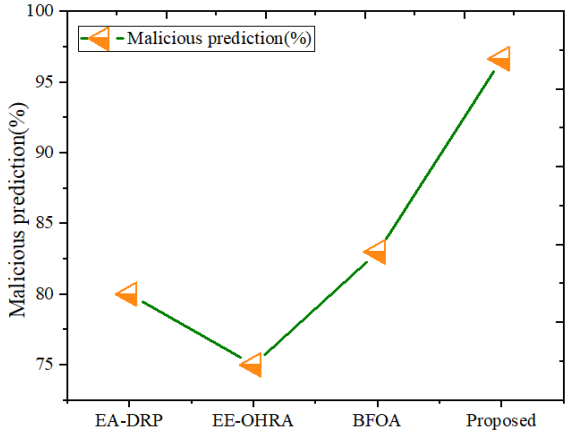

Fig.16. Comparison of Malicious Prediction Accuracy

The malicious node prediction accuracy is shown in Fig. 16. Compared to other techniques, the proposed method achieves significantly higher prediction accuracy. The overall malicious prediction accuracy reaches 96.66%. Table 3 presents a comparative analysis of existing methods.

Table 3. Comparative Analysis of Existing Methods

Methods	Throughput (bps)	Energy consumption (mJ)	Delay (ms)	Malicious prediction (%)
EA-DRP	0.64	0.24	0.007	80
EE-OHRA	0.45	0.22	0.004	75
BFOA	0.70	0.12	0.0035	83
Proposed	0.95	0.08	0.002	96.66

5.3. Discussion

The primary objective of the proposed model was to enhance secure and efficient routing. A comparative analysis was conducted to verify the efficiency improvements of the proposed method. To address the limitations of existing protocols, the proposed method employs the Hummingbird Optimization Algorithm. Consequently, the proposed approach enhances wireless network security against malicious activities. The overall performance of the proposed approach is summarized in Table 4.

Table 4. Overall Performance of HBbGBBTMN

Metrics	Performance
Energy consumption	0.08 mJ
Throughput	0.95 bps
Packet delivery ratio	99%
Packet drop	0.07%
Delay	0.002 ms
Malicious prediction	96.66%

The outstanding performance of the proposed model is demonstrated by comparing it with alternative methods. The performance of the proposed approach is evaluated using the following metrics: delay, PDR, throughput, packet drop rate, energy consumption, and malicious node detection accuracy. Compared to existing methods, the proposed method yields superior results. The proposed HBbGBBTMN model performed effectively, achieving a 99% packet delivery ratio, 0.95 bps throughput, 0.07% packet loss, 96.66% prediction accuracy, 0.002 ms delay, and 0.08 mJ energy consumption. Thus, the proposed technique is suitable for secure and efficient routing in WSNs.

6. Conclusions

For 5G-enabled WSN routing, the proposed approach provides an intelligent, secure, and energy-efficient routing solution. The proposed approach reduces energy consumption, optimizes routes, and identifies and isolates malicious nodes using an improved Hummingbird fitness function and a Bernoulli-Binomial trust assessment. Validated by key metrics including PDR, throughput, packet loss, malicious node detection, and delay, this method enhances network performance and reliability, confirming its robustness in dynamic networks. Furthermore, the novel HBbGBBTMN technique was compared with existing protocols, including EA-DRP, EE-OHRA, BFOA, DCCP, PPI, NoDPCC, and IVSP, demonstrating superior performance. Simulations using a Constant Bit Rate (CBR) model were conducted to ensure accurate performance evaluation. Finally, the proposed method achieved a 99.3% packet delivery ratio, 0.95 bps throughput, 0.07% packet loss, 96.66% prediction accuracy, 0.002 ms delay, and 0.08 mJ energy consumption. Future research may focus on developing multiple trusted routing paths to further improve energy efficiency.

All the Declarations and Statements

Author Contributions Statement

Sachin B M – Writing – Drafted the initial manuscript, contributed to the literature survey, and documented the technical background of the study.
Dr. Mrinal Sarvagya – Writing – Review and Editing, and Project Management: Reviewed and edited the manuscript, ensured clarity and coherence, and helped coordinate project milestones and deadlines.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Data Availability Statement

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Ethical Declarations

Ethical approval is not required as no human subjects or animals were involved in this study.

Acknowledgments
None

Declaration of Generative AI in Scholarly Writing
AI and AI-assisted technologies were not used during the writing process.

Abbreviations
The following abbreviations are used in this manuscript:

WSN - Wireless Sensor Networks
HBbGBBTMN - Hummingbird-based Graph Bernoulli Binomial Trust Management Network
IoT - Internet of Things
CEEPR - collaborative energy-efficient routing protocol
MOISA - multi-objective improved seagull algorithm
RPL - Routing Protocol for Low-Power and Lossy Networks
PDR - packet delivery ratio
HBO - Hummingbird Optimization
EA-DRP - Energy Aware on Demand Routing Protocol
EE-OHRA - Efficient Optimized hierarchical Routing Algorithm
BFOA - Bacterial Foraging Optimization Algorithm
DCCP - Distributed Congestion Control Protocol
PPI - Packet Priority Intimation
IVSP - Intelligent Video Surveillance Platform

Appendix
Implication: The proposed HBbGBBTMN algorithm is essential for enhancing the efficiency of 5G-enabled WSNs. The integration of energy-efficient optimization and trust-based decisions, along with continuous malicious node detection, improves security and energy efficiency in 5G routing. This enhances the efficiency of critical applications such as smart cities, industrial IoT, health monitoring, and autonomous transport, where reliable data transfer and security are paramount. Moreover, the application of probabilistic trust evaluation and intelligent optimization minimizes packet loss and maximizes network lifetime, making this model suitable for large-scale decentralized networks.

Reference

[1] M. J. Al-Dujaili, M. A. Al-Dulaimi, “Fifth-generation telecommunications technologies: Features, architecture, challenges and solutions,” *Wireless Personal Communications*, vol. 128, no. 1, pp. 447-469, 2023. https://doi.org/10.1007/s11277-022-09962-x

[2] Y. Zhang, Y. Liu, L. Guo, J.Y. Lee, “Measurement of a large-scale short-video service over mobile and wireless networks,” *IEEE Transactions on Mobile Computing*, vol. 22, no. 6, pp. 3472-3488, 2022. DOI: 10.1109/TMC.2021.3139893

[3] L. Mei, J. Gou, Y. Cai, H. Cao, Y. Liu, “Real-time mobile bandwidth and handoff predictions in 4G/5G networks”, *Computer Networks*, vol. 204, pp. 108736, 2022. https://doi.org/10.1016/j.comnet.2021.108736

[4] L. Bojic, “Metaverse through the prism of power and addiction: what will happen when the virtual world becomes more attractive than reality?,” *European Journal of Futures Research*, vol. 10, no. 1, pp. 22, 2022. https://doi.org/10.1186/s40309-022-00208-4

[5] A. Bagwari, J. Logeshwaran, M. Raja, P. Devisivasankari, J. Bagwari, V. Rathi, A.M.E. Saad, “Intelligent computational model for energy efficiency and AI automation of network devices in 5G communication environment,” *Tsinghua Science and Technology*, vol. 29, no. 6, pp. 1728-1751, 2024. DOI: 10.26599/TST.2024.9010005

[6] I. Ullah, H. El Sayed, S. Malik, M.A. Khan, “Performance evaluation of quality of experience aware mobility management in heterogeneous cellular networks,” *IEEE Access,* 2024. DOI: 10.1109/ACCESS.2024.3426991

[7] K. Khujamatov, N. Akhmedov, E. Reypnazarov, D. Khasanov, A. Lazarev, “Device-to-device and millimeter waves communication for 5G healthcare informatics,” In *Blockchain Applications for Healthcare Informatics,* pp. 181-211. Academic Press, 2022. https://doi.org/10.1016/B978-0-323-90615-9.00019-0

[8] W. Jiang, B. Han, “Evolution to Fifth-Generation (5G) Mobile Cellular Communications,” In Cellular communication networks and standards: The evolution from 1G to 6G, pp. 149-168. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-57820-5_9

[9] J.L. Frauendorf, É. Almeida de Souza, “The different architectures used in 1G, 2G, 3G, 4G, and 5G networks,” In *The architectural and technological revolution of 5G,* pp. 83-107. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-031-10650-7_7

[10] V.V. Logvinov, S.M. Smolskiy, “Systems and networks of wireless communication,” In *Radio Receivers for Systems of Fixed and Mobile Communications,* pp. 51-119. Cham: Springer International Publishing, 2022. https://doi.org/10.1007/978-3-030-76628-3_2

[11] H.M.A. Fahmy, “WSNs applications,” In *Concepts, applications, experimentation and analysis of wireless sensor networks,* pp. 67-242. Cham: Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-20709-9_3

[12] H. N. Vishwas, T. K. Ramesh, "Recent Trends in Localization, Routing, and Security for Wireless Sensor Networks," IEEE Access, 2025. DOI: 10.1109/ACCESS.2025.3555280
[13] Z. Chen, Z. Zhang, Z. Yang, "Big AI models for 6G wireless networks: Opportunities, challenges, and research directions," *IEEE Wireless Communications*, 2024. DOI: 10.1109/MWC.015.2300404
[14] M. Banafaa, I. Shayea, J. Din, M.H. Azmi, A. Alashbi, Y.I. Daradkeh, A. Alhammadi, "6G mobile communication technology: Requirements, targets, applications, challenges, advantages, and opportunities," *Alexandria Engineering Journal*, vol. 64, pp. 245-274, 2023. https://doi.org/10.1016/j.aej.2022.08.017
[15] G. Arya, A. Bagwari, D.S. Chauhan, "Performance analysis of deep learning-based routing protocol for an efficient data transmission in 5G WSN communication," *IEEE Access*, vol. 10, pp. 9340-9356, 2022. DOI: 10.1109/ACCESS.2022.3142082
[16] M.S. Alzaidi, P.K. Shukla, V. Sangeetha, K.N. Pandagre, V.K. Minchula, S. Sharma, V. Prashanth, "Applying machine learning enabled myriad fragment empirical modes in 5G communications to detect profile injection attacks," *Wireless Networks*, vol. 30, no. 6, pp. 5533-5546, 2024. https://doi.org/10.1007/s11276-023-03301-z
[17] M.K. Roberts, P. Ramasamy, "An improved high performance clustering based routing protocol for wireless sensor networks in IoT," *Telecommunication Systems*, vol. 82, no. 1, pp. 45-59, M.K. Roberts, P. Ramasamy, "An improved high performance clustering based routing protocol for wireless sensor networks in IoT," Telecommunication Systems, vol. 82, no. 1, pp. 45-59, 2023. https://doi.org/10.1007/s11235-022-00968-1
[18] U. Panahi, C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," *Ain Shams Engineering Journal*, vol. 14, no. 2, pp. 101866, 2023. https://doi.org/10.1016/j.asej.2022.101866
[19] A.U. Rehman, I. Mahmood, M. Kamran, M. Sanaullah, A. Ijaz, J. Ali, M. Ali, "Enhancement in Quality-of-Services using 5G cellular network using resource reservation protocol," *Physical Communication*, vol. 55, pp. 101907, 2022. https://doi.org/10.1016/j.phycom.2022.101907
[20] T. Kavitha, N. Pandeeswari, R. Shobana, V.R. Vinothini, K. Sakthisudhan, A. Jeyam, A.J.G. Malar, "Data congestion control framework in Wireless Sensor Network in IoT enabled intelligent transportation system," *Measurement: Sensors*, vol. 24, pp. 100563, 2022. https://doi.org/10.1016/j.measen.2022.100563
[21] J.M. Jorquera Valero, P.M. Sánchez Sánchez, A. Lekidis, J. Fernandez Hidalgo, M. Gil Pérez, M.S. Siddiqui, G. Martínez Pérez, "Design of a security and trust framework for 5G multi-domain scenarios," *Journal of Network and Systems Management*, vol. 30, no. 1, pp. 7, 2022. https://doi.org/10.1007/s10922-021-09623-7
[22] F. Salahdine, Q. Liu, T. Han, "Towards Secure and Intelligent Network Slicing for 5G Networks," *IEEE Open Journal of the Computer Society*, vol. 3, pp. 23-38, 2022. DOI: 10.1109/OJCS.2022.3161933
[23] I. Zografopoulos, N.D. Hatziargyriou, C. Konstantinou, "Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations," *IEEE Systems Journal*, vol. 17, no. 4, pp. 6695-6709, 2023. DOI: 10.1109/JSYST.2023.3305757
[24] P.K. Roy, A. Bhattacharya, "SDIWSN: A software-defined networking-based authentication protocol for real-time data transfer in industrial wireless sensor networks," *IEEE Transactions on Network and Service Management*, vol. 19, no. 3, pp. 3465-3477, 2022. DOI: 10.1109/TNSM.2022.3173975
[25] A. Irshad, M. Alreshoodi, "SEMS-5G: A Secure and Efficient Multi-Server Authentication Scheme for 5G Networks," *IEEE Access,* 2024. DOI: 10.1109/ACCESS.2024.3381616
[26] H.L. Gururaj, R. Natarajan, N.A. Almujally, F. Flammini, S. Krishna, S.K. Gupta, "Collaborative energy-efficient routing protocol for sustainable communication in 5G/6G wireless sensor networks," *IEEE Open Journal of the Communications Society*, vol. 4, pp. 2050-2061, 2023. DOI: 10.1109/OJCOMS.2023.3312155
[27] A. Wakili, S. Bakkali, A.E.H. Alaoui, "Machine learning for QoS and security enhancement of RPL in IoT-Enabled wireless sensors," Sensors International, vol. 5, pp. 100289, 2024. https://doi.org/10.1016/j.sintl.2024.100289
[28] M. Shanmathi, A. Sonker, Z. Hussain, M. Ashraf, M. Singh, M. Syamala, "Enhancing wireless sensor network security and efficiency with CNN-FL and NGO optimization," *Measurement: Sensors*, vol. 32, pp. 101057, 2024. https://doi.org/10.1016/j.measen.2024.101057
[29] C. Li, J. Wu, Z. Zhang, A. Lv, "Energy-harvesting Q-learning secure routing algorithm with authenticated-encryption for WSN," *ICT Express*, vol. 9, no. 6, pp. 1077-1084, 2023. https://doi.org/10.1016/j.icte.2023.05.006
[30] S.K. Sharma, M. Chawla, "PRESEP: Cluster based metaheuristic algorithm for energy-efficient wireless sensor network application in internet of things," *Wireless Personal Communications*, vol. 133, no. 2, pp. 1243-1263, 2023. https://doi.org/10.1007/s11277-023-10814-5
[31] U. Srilakshmi, S.A. Alghamdi, V.A. Vuyyuru, N. Veeraiah, Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260-14269, 2022. DOI: 10.1109/ACCESS.2022.3144679
[32] U. Majeed, A.N. Malik, N. Abbas, W. Abbass, "An energy-efficient distributed congestion control protocol for wireless multimedia sensor networks," *Electronics*, vol. 11, no. 20, pp. 3265, 2022. https://doi.org/10.3390/electronics11203265

Authors' Profiles

Sachin B. M. received his Bachelor of Engineering in Electronics and Communication Engineering from Visvesvaraya Technological University in 2009 and his M.Tech in Digital Electronics and Communication from Visvesvaraya Technological University in 2011. He has been associated with the Department of Electronics and Communication Engineering at Bangalore Institute of Technology since 2015. His research interests include Wireless Sensor Networks and Digital Communication, and he is currently pursuing his Ph.D. at REVA University, Bengaluru. He has been involved in organizing academic programs, supervising undergraduate and postgraduate projects, and participating in seminars, workshops, and Faculty Development Programs (FDPs). His areas of teaching include Analog Electronic Circuits, Analog Communication, Principles of Communication Systems, Digital Communication, Microwave Engineering, Antenna and Wave Propagation, and Wireless Sensor Networks.

Dr. Mrinal Sarvagya is a Professor in the School of Electronics and Communication Engineering. She received her PhD degree in Wireless Communication from IIT Kharagpur, her MTech degree in Digital Communication (course work from IIT Kanpur) from DAVV Indore, and her BE degree in Electronics and Communication Engineering from Govt. Engineering College Ujjain. She received the best thesis award from IIT Kharagpur in 2009 for her thesis titled "QoS based packet scheduling and resource allocation schemes for WCDMA UMTS". She is a member of professional bodies WIE and IEEE. She has 20 years of teaching experience, teaching subjects including Wireless Communication, Advanced Digital Communication, Computer Communication and Networking, Real-Time Operating Systems, Ad Hoc Wireless Networks, and Protocol Engineering. Her research interests include Wireless Communication, channel equalization in OFDM-IDMA/SCM receivers, and Cognitive Radio Networks. She served as Principal Investigator for VGST Karnataka "Zero padding OFDM signals for Cognitive Radio Networks" (2012-2014) and for IEEE Hyderabad "Multimedia Communication over Fibre Optical link" (2012), exhibited at Birla Science Museum Hyderabad. She is currently Principal Investigator for a sponsored project from the Naval Research Board, Ministry of Defence, India (2015), and served as Principal Investigator for the project titled "Attitude determination of Ship in floating dry dock" sponsored by ISRO, India (2019). Her name is included in Marquis Who's Who in the World directory from 2007 onwards. She has received many awards, including the Young Research Scientist award from VGST Karnataka in 2013 and the Bharat Jyoti Award from the International Friendship Society of India. She received the Outstanding Faculty in Engineering Award from the Venus International Foundation, India, in 2017, and the Best Researcher Award 2020 from REVA University. She has more than 105 publications in international journals and conferences, and is a selection panel member for the Association of Commonwealth Universities fellowships, UK.

How to cite this paper

Sachin B. M., Mrinal Sarvagya, " An Improved Trust-based and Energy Efficient Secure Routing Protocol for 5G-WSN", International Journal of Information Technology and Computer Science(IJITCS), Vol.18, No.4, pp.68-84, 2026. DOI:10.5815/ijitcs.2026.04.05