Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 6s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Optimal Cluster Head Selection and Reliable Routing Using Enhanced Butterfly Optimization and Improved Dynamic Source Routing Protocol Over Hybrid Networks

Mr. P. Balamuthukumar[1], Dr. V. Kathiresan[2]

[1]Research Scholar, Park's College, Tirupur, Tamilnadu, India.

[2]Associate Professor & Principal, A.V.P. College of Arts and Science, Tirupur, Tamilnadu, India.

Cite this paper as: Mr. P. Balamuthukumar, Dr. V. Kathiresan, (2025) Optimal Cluster Head Selection and Reliable Routing Using Enhanced Butterfly Optimization and Improved Dynamic Source Routing Protocol Over Hybrid Networks. *Journal of Neonatal Surgery*, 14 (6s), 1-10.

ABSTRACT

The integration of Internet of Things (IoT), Mobile Ad-hoc Networks (MANETs), and Wireless Sensor Networks (WSNs) under a unified cloud-based system presents unique challenges and opportunities for optimizing network functionality and scalability. This integration aims to leverage the strengths of each technology IoT's extensive connectivity, MANET's flexible topology, and WSN's efficient local data collection and monitoring to create a robust, scalable, and efficient network system capable of dynamic data processing and enhanced decision-making. Still, the existing system has problem with lower packet delivery ratio since inappropriate Cluster Head (CH) node selection process. To address the aforementioned issue, in this work, an innovative approach using Enhanced Butterfly Optimization (EBO) and Improved Dynamic Source Routing (IDSR) protocol is proposed for optimal CH node selection and reliable routing in heterogeneous networks. Initially, the hybrid system model is constructed via sensor nodes, MANET nodes, IoT sensor nodes and cloud server. This methodology leverages the EBO algorithm to strategically select CHs based on a composite metric that considers energy efficiency, delay, throughput and lifetime metrics, thus ensuring sustainable network operation and reduced energy consumption. Concurrently, the IDSR protocol has been tailored to address the dynamic and ad-hoc nature of IoT and MANET communications, incorporating enhanced security measures and trust-based routing to mitigate spoofing attacks and ensure data integrity. Between sensors in the Internet Cloud, MANET is establishing the faster and most reliable path. Extensive simulations demonstrate that our integrated approach significantly outperforms traditional methods in terms of end to end delay, energy consumption, network longevity, data throughput, and security, confirming its effectiveness in optimizing network operations across diverse deployment scenarios.

Keywords: *Heterogeneous network, IoT, MANET, cloud, Enhanced Butterfly Optimization (EBO), Improved Dynamic Source Routing (IDSR).*

1. INTRODUCTION

MANET offers significant opportunities for research and the development of wireless network applications. In recent years, the sector of wireless communication has seen tremendous expansion Ad-hoc networks represent an innovative and rapidly evolving research domain. These networks can function independently or connect to other networks or the Internet through multiple access points, enabling the creation of cutting-edge applications [1]. Their potential applications include road safety management, home monitoring, healthcare systems, disaster recovery, defense operations, weapon control, and robotics.

The IoT framework is vast and highly intricate, usually made up of actuators, sensors, and gateways in the tens of thousands. While gateways connect to the protocols used by cloud-based services and the Internet are equally varied, devices interact with gateways using a variety of protocols. Data processing in this intricate architecture is done by a variety of diverse organizations. Ensuring the integrity, security, and transfer of data are important factors [2]. Consequently, to manage data access, protocols and technologies are necessary, securing information, and ensuring efficient data flow. In recent years, extensive research has been conducted to address security challenges within the IoT paradigm. Some studies focus on specific layers of the architecture, while others strive to achieve end-to-end security [3] [4]. Additionally, there have been many suggested techniques and processes, emphasizing energy efficiency and extending the lifespan of IoT networks.

Security and energy management are two significant challenges in Wireless Sensor Networks (WSNs). These networks are commonly implemented in difficult regions with unreliable communication lines and include a significant number of widely separated sensor nodes. The diversity of devices, protocols, routing methods, and services within WSNs makes implementing

conventional IT network solutions exceedingly difficult [5][6]. Consequently, many existing security mechanisms are either inadequate or incompatible. To attain certain security levels while minimizing costs for low-power, resource-constrained devices, a variety of techniques have been used, including trust management and lightweight encryption approaches. WSN routing systems are still vulnerable to major risks, nevertheless, such fraudulent or fake routing information being introduced, which may cause delays or packet losses because of routing conflicts [7]. To mitigate these risks, there are techniques to stop routing attacks, include information correlation across several nodes and encryption.

To ensure secure and dependable information sharing in contemporary MANETs, this work attempts to develop an energy-efficient routing protocol. To increase the efficiency of energy and increase network lifetime, and improve scalability in densely populated areas, a clustering approach can be employed. Additionally, using multiple node-disjoint paths contributes to reliability, stability, and network robustness [8]. Ensuring the security of MANETs while minimizing delays requires addressing malicious attacks. Compared to fixed networks, MANETs have greater packet losses and delays because of their dynamic and unstable architecture. Energy-saving techniques are essential since mobile nodes depend on a limited amount of battery power, improve network efficiency, and prolong network lifespan. With unrestricted mobility and the ability to connect without centralized control, MANET nodes collaboratively manage the network and routing tasks. However, these characteristics make MANETs more vulnerable to routing and security challenges than traditional networks [9]. Thus, developing effective mechanisms to address mobility-related issues is essential when making routing decisions.

Similarly, routing in hybrid networks composed of IoT, MANETs, and WSNs presents unique challenges. The dynamic nature of these networks, particularly with the mobility inherent in MANETs and the varying sensor deployment in WSNs, requires a flexible yet robust routing protocol. Conventional static routing protocols are incapable of handling the high degree of network topology changes and diverse traffic patterns, necessitating the development of an improved dynamic routing protocol that can ensure reliability and security while accommodating the fluid network structures. This paper introduces the Enhanced Butterfly Optimization (EBO) algorithm for effective CH node selection and the Improved Dynamic Source Routing (IDSR) protocol for reliable routing. The EBO algorithm is tailored to the specific requirements of hybrid networks by incorporating a fitness function that evaluates potential CH according to their connectedness, energy levels, and distance from other nodes. This method reduces energy usage across the network while also extending its operational life.

The contributions of this research are twofold: firstly, it proposes a novel CH selection algorithm that optimizes key performance metrics across IoT, MANETs, and WSNs; secondly, it enhances a well-established routing protocol to increase reliability and security in dynamic network topologies. The following is how this paper is organized: A review of relevant studies is given in Section II, Section III describes the system model and underlying assumptions., the results of the experiments are discussed in Section V, the CH node selection and routing procedures are explained in Section IV, and the article is concluded in Section VI.

2. LITERATURE SURVEY

In [10], Hussein et al (2022) it was suggested that preserving for wireless sensor networks (WSNs) to maintain communication integrity, a rapid dependable, secure way to distribute and manage keys is required. An appreciated cluster-based routing protocol in WSNs, the Low Energy Adaptive Clustering Hierarchy (LEACH) algorithm, has also been enhanced to improve energy efficiency, simplicity, and load-balancing capabilities to maximize energy use. To provide secure node communication, this work uses elliptic curve cryptography in conjunction with distributed key exchange and management mechanisms. An enhanced routing protocol that is based on the LEACH algorithm is also presented, showing better results in terms of dead nodes, energy usage, and network lifespan.

In [11], Narendran, M., and Periyasamy Prakasam (2019) an emphasis on residual energy and the randomized selection of nodes that have not been previously identified as CHs in previous rounds, an energy-efficient method for CH election in mobile WSNs is put forward, examined, and assessed. In contrast to more conventional clustering techniques like Lower ID (LID), the research uses a Random Competition-Based Clustering (RCC) approach, which shows higher stability. There is also discussion of the Invasive Weed Optimization (IWO) algorithm, a recently developed metaheuristic that draws inspiration from weed behavior. Premature convergence may result from seeds clustering close to the top-performing weed due to the spatial dispersion operators and reproduction processes of the original IWO.

In [12], Aroulanandam et al (2020) it was highlighted that MANET nodes are often connected to various applications involving substantial data exchange. MANET optimization uses specific load-balancing techniques to improve the dependability of application services. The present study combines Learning-based Routing (LR) with the Dynamic Range Clustering (DRC) method to enhance the network's data management and energy efficiency. To provide effective and congestion-free data flow, the LR algorithm identifies unique nearby nodes, while the DRC method chooses cluster heads and preserves cluster stability. There have been attempts to improve network performance in a variety of traffic scenarios by combining these two normally incompatible techniques.

In [13], Maheshwari et al (2021) increasing the network's longevity and reducing total energy usage are the main objectives. To increase network lifetime, WSNs now make considerable use of clustering and routing methods. To choose the best

cluster head from a collection of nodes, this research uses the Butterfly Optimization Algorithm (BOA). A number of parameters, including the nodes' degree, centrality, distance from optimizing the selection process is based on the base station, neighbors, and residual energy. Ant Colony Optimization (ACO) takes into perspective factors such distance, residual energy, and node degree to find the best path between the cluster head and the base station. Metrics used to assess the technique's effectiveness include energy consumption, the number of resident and dead nodes, and the volume of data packets received by the base station.

In [14], Benakappa, S. M., and M. Kiran (2022) two crucial factors were used in the proposal of the Trust-Based Energy-Aware Multipath Disjoint Routing Protocol (TEA-MDRP) for MANETs to determine the best path between source and destination nodes: Accumulated Trust Value (ATV) and residual energy ($Nres$) of the nodes. The ATV is determined based on a node's packet forwarding performance, indicating its reliability in forwarding data. TEA-MDRP prioritizes nodes with high ATV and adequate residual energy for route selection. A high ATV reflects the node's trustworthiness in packet forwarding, while sufficient residual energy minimizes the likelihood of frequent path disruptions and packet losses. Consequently, TEA-MDRP enhances both network and path longevity, while also improving communication throughput. Moreover, by relying on legitimate nodes with stable paths, the protocol significantly reduces control packet overhead caused by repeated route rediscovery processes.

In [15], Krishnamoorthy et al (2023) in IT technology, the combination of IoT, WSN, and MANET produces a complex heterogeneous network that presents new difficulties. In this network, MANET uses Energy Saving Optimization (ESO) to provide a dependable path between sensor nodes and gateway nodes in the IoT context. This approach helps conserve energy at each node while lowering operational costs. In terms of parameters like throughput, packet delivery ratio, routing overhead, residual energy, and the number of existence nodes, the suggested approach performs better than the others, according to the results of the ns-3 simulations.

3. PROPOSED METHODOLOGY

The network that is the focus of this research consists of cloud server, sensor nodes, MANET nodes, and IoT sensor nodes. Heterogeneous network characteristics are introduced when MANET and WSN are integrated inside an IoT framework. The IoT nodes are capable of gathering, controlling, and monitoring environmental data. Additionally, Susceptible (S), Exposed (E), Infectious (I), Recovered (R), and Failed (F) nodes are all part of the system. This setup enhances trust and ensures effective communication among sensor nodes. The gathered data the Internet of Things environment is processed and stored in the cloud design. This study suggests using the Enhanced Butterfly Optimization (EBO) method for cluster formation and Cluster Head (CH) selection in IoT-based WSNs. The Improved Dynamic Source Routing (IDSR) protocol in MANET is then used for spoofing attack detection and short path routing. This is the in general block diagram for the system that is being suggested. The primary block diagram for the suggested system is shown in Fig. 1.

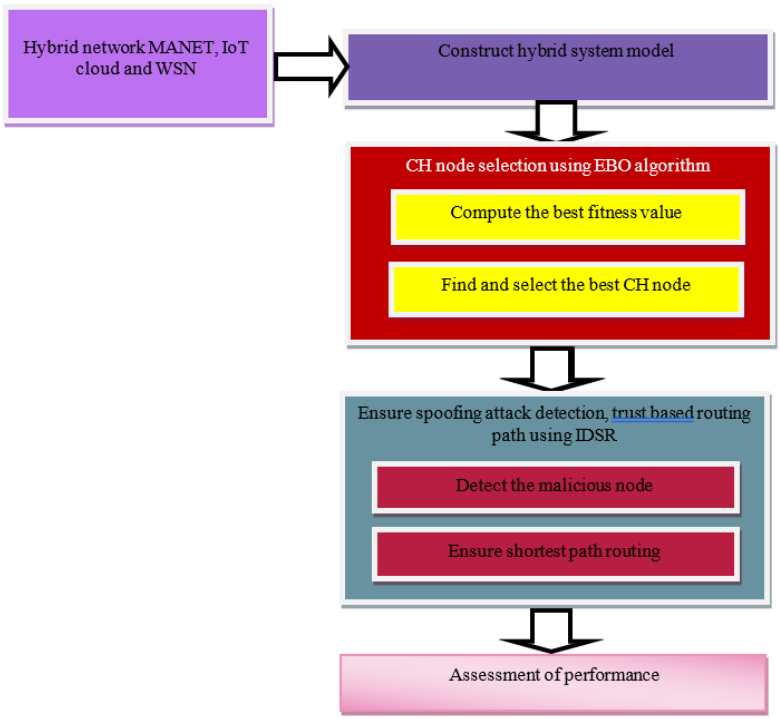

Fig 1 General block diagram for the system that is proposed

3.1 Construct hybrid system model

In constructing a detailed description of a hybrid network model incorporating sensor nodes (WSN), MANET nodes, IoT sensor nodes, and a cloud server, it's essential to delineate the operational framework, data flow, node characteristics, and network behavior using mathematical models and diagrams to better illustrate the concepts.

Below is a comprehensive breakdown:

The network consists of several different types of nodes, each fulfilling specific roles:

- **Sensor Nodes (WSN):** These nodes are primarily responsible for gathering environmental data.
- **MANET Nodes:** Networks made up of mobile nodes without the need for a fixed infrastructure.
- **IoT Sensor Nodes:** Advanced nodes that can process some data and connect directly to the internet or cloud servers.
- **Cloud Server:** Centralized servers that process and store data collected from all nodes.

Node States (SEIRF Model):

- **Susceptible Nodes (S)**: Operating nodes that are susceptible to security threats or malfunctions.
- **Exposed Nodes (E)**: Nodes that are not yet infectious but have been compromised or are at high risk.
- **Infectious Nodes (I)**: Nodes that are actively compromised and can affect other nodes.
- **Recovered Nodes (R)**: Nodes that were compromised but have been secured and restored to full functionality.
- **Failed Nodes (F)**: Nodes that have ceased functioning due to hardware failures, security breaches, or other critical issues.

Trust and Communication:

- Incorporating trust models to evaluate and enhance the reliability of nodes, especially in an IoT environment where nodes may enter and leave the network on a regular basis.
- Trust metrics can be used to decide which nodes participate in the network and which are isolated to prevent the spread of failures or malicious activities.

In an IoT environment, MANET enhances trust and facilitates seamless intercommunication among sensor nodes. IoT combines internet services with WSN technology, supporting the growing interconnected world of electronic devices and intelligent network applications. IoT sensors continuously convert physical phenomena into digital data at various time intervals. However, uncertainties in sensor nodes lead to problems including increased data transmission times and greater power usage. The proposed model addresses these issues by improving throughput and reducing energy consumption. Through the development of trust and the selection of the most efficient routes, this MANET algorithm improves network performance. As illustrated in Fig. 2, various sensor nodes connect to nearby mobile nodes, which subsequently form clusters based on the high density of sensors within the network.

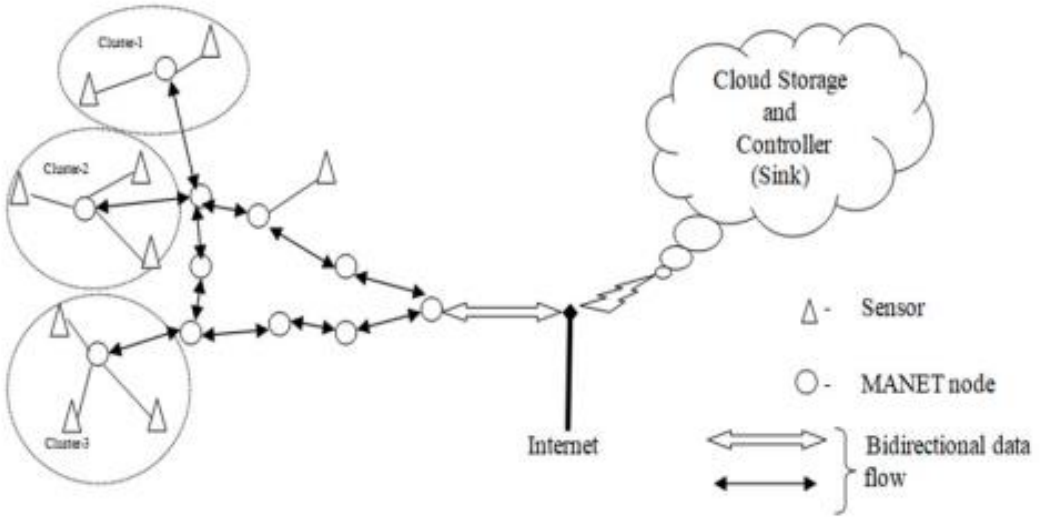

Fig 2 Internet-Based Heterogeneous Network Built with Sensors, MANETs, and Cloud Storage

The sensors are managed, observed, and data is collected by the CH. In the network, the CH fluctuates according on the distance between the sensor and the mobile node, in addition to the node's energy level. Data is sent to the gateway node in MANET via an internet-based cloud network that includes the CH, nearby nodes, and gateway nodes. The routing process in MANET optimizes energy consumption while ensuring reliable route paths. The proposed model sequentially establishes available and optimal routes. Additionally, MANET facilitates data transmission, storage, and command reception through internet services, creating a heterogeneous network for using gateways to transmit data between cloud systems and MANETs. MANET connects to the cloud routing algorithm via gateway nodes. as using MANET-EBO, the network achieves optimal metrics including throughput, energy efficiency, delay reduction, packet delivery ratio, and minimum routing overhead, resulting in more overall performance as compared to a simple IoT network.

3.2 Cluster formation and Cluster Head (CH) node selection using Enhanced Butterfly Optimization (EBO) algorithm in IoT based WSN

This study uses the best CH selection method by employing EBO algorithm over IoT based WSN. It is based on energy, delay, throughput and lifetime metrics. EBO algorithm is used to produce optimal solutions which improve the network's speed and energy efficiency. The best fitness values are generated via objective function which is to provide efficient packet transmission over IoT based WSN. Clustering techniques help manage the challenges posed by large network sizes, regulate traffic, and enhance the energy efficiency of individual nodes. Faulty nodes within a cluster can be quickly detected and replaced automatically using an appropriate algorithm. In a clustered network, the graphical representation is denoted as G (N, E). E is the total amount of energy needed by the node to transmit the packet $i\ to\ j\ and\ i,j\ \in\ N$ is the number of nodes in the cluster. The CH energy is calculated using the node E_{Ri} residual energy. The distance d_{ij} is equal to the packet's velocity to the time needed to deliver every packet from i to j, and the residual energy E_{Ri} is computed by dividing the node's total energy by its consumed energy. E_p is the energy needed to send one packet, and P_n is the total number of packets.

$$E_{CH} = \frac{E_{Ri}}{\sum_{j=1}^{n}((d_{ij}+(E_p \times P_n))} \quad (1)$$

The network carefully monitors the mobility of data packets as they are sent between sensor nodes. Specifically, the network's data throughput is measured by the volume of data that is successfully sent from the source to the destination per second.

In IoT-based WSNs, the efficiency of network operations is paramount. This efficiency is predominantly influenced by how well the network manages its energy resources, handles delays, optimizes throughput, and extends its operational lifetime. Traditional methods of CH selection often fail to simultaneously optimize these critical metrics, leading to suboptimal network performance. This necessitates a robust optimization technique capable of handling multiple objectives. The natural foraging behaviors of butterflies served as the model for the EBO algorithm [16]. It utilizes sensory modality and fragrance (pheromone) intensity to search for optimal solutions in a multidimensional space. For CH selection in IoT-based WSNs, the EBO algorithm has been adapted to consider energy consumption, delay, throughput, and network lifetime as key metrics for fitness evaluation.

The fitness of a potential CH is evaluated based on a weighted sum of several key performance indicators:

$$Fitness(CH) = w_1 \cdot EnergyEfficiency(CH) + w_2 \cdot Delay(CH) + w_3 \cdot Throughput(CH) + w_4 \cdot Lifetime(CH), \quad (2)$$

where w_1, w_2, w_3, w_4 are weights given to each measure that represent the significance they are in relation to the network's operational objectives.

In this work, CH is selected by EBO to select the optimal CH nodes over IoT based WSN. The EBO algorithm is a novel nature-inspired approach that emulates the food-seeking (minimizing energy consumption using selected sensor nodes) and mating behaviors of butterflies to address energy efficiency challenges in hybrid networks. This algorithm primarily relies on using their excellent sense of smell, butterflies forage optimally selects nodes and identify the location of nectar partners. Scientific studies have revealed that butterflies possess a highly precise ability to detect fragrance sources, which aligns with the process of Cluster Head (CH) node selection.

Butterfly scent intensity reflects fitness (CH node selection). Fitness varies as the butterfly moves. The three main ideas of sensory modality (c), stimulus intensity (I), and power exponent (a) for optimal node selection guide the whole sensing and processing process in the Enhanced Butterfly Optimization (EBO) method [17]. For the selection of sensor nodes from the IoT-based WSN, *I* connected with fitness (lower energy usage) in the EBO Algorithm. Equation (3) uses these ideas to define the scent in the EBO Algorithm as according to the intensity of physical stimulus.

$$f = cI^a \quad (3)$$

The sensory modality, c, is produced by using less energy, the power exponent depends on the modality, whereas the stimulus intensity is in, and f is the perceived magnitude of the scent, or how intensely other butterflies experience it. The range [0,1] is therefore a & c. In addition, if a = 0, The other butterflies could thus be unable to detect the fragrance of any butterfly. This means that the parameter a controls the behavior of the algorithm. The pace at which the EBO algorithm converges is also determined by C, another important parameter. The following is an idealized version of the aforementioned butterfly traits to use a search algorithm to demonstrate the previously discussed topics:

1. All butterflies are assumed to release a fragrance that allows them (nodes) to attract one another (nodes).
2. The butterflies may travel at random or are drawn to the one that fragrance the strongest.
3. The butterfly's stimulus intensity is defined or influenced by the target function's landscape.

Initialization, iteration, and finalization are the three steps in which the Enhanced Butterfly Optimization (EBO) algorithm works. An iterative search for the best CH nodes follows the initialization step at the start of each algorithm operate. In the final phase, the algorithm concludes once the most optimal solution is identified. During the initialization phase, the EBO algorithm calculates energy consumption and defines the solution space. Parameter values required for the algorithm are assigned, and along with their corresponding a fragrance and fitness values, the positions of butterflies (sensor nodes) are started at random inside the CH node selection search space. The algorithm moves onto the iteration phase when the startup step is finished. Each butterfly in the CH node selection solution space updates its position throughout each iteration, and their energy consumption values are assessed. First, the fitness values of all sensor nodes at various positions in the solution space are calculated. Subsequently, the butterflies emit fragrance at their respective positions, as determined by equation (3). The node becomes closer to the optimal nodes, or fittest solution g*, throughout the global search phase, as shown by equation (4).

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i * ECE_W \quad (4)$$

At each iteration number t, where x_i^t is the solution vector x_i for the ith node. In this case, g^* represents the node solution with the highest rating among all the solutions in the current iteration. As the ith butterfly, f_i and r∈[0,1] reflect its fragrance. is a number that is chosen at random. Equation (5) may be used to describe the local search phase,

$$x_i^{t+1} = x_i^t + \left(r^2 \times x_j^t - x_k^t\right) \times f_i * ECE_W \quad (5)$$

In the CH node selection solution space, the jth and kth butterflies are denoted by x_j^t and x_k^t, respectively. Given a random integer r∈[0,1] and x_i^t and x_k^t belonging to the same swarm, equation (5) develops into a local random walk. To select nodes from the hybrid network as efficiently as possible, butterflies search for food and partners on both a local and global scale. Global search may be changed to more concentrated local search using the EBO algorithm's switch probability p. Until the stoppage conditions are satisfied, the iteration phase keeps going. The method returns the optimal solution and its greatest fitness value at the end of the iteration phase. The EBO method is used in equations (4) and (5) to determine the ideal number of nodes for the network by including node weight. Through the best possible CH node selection across the hybrid network, the EBO algorithm aims to improve energy efficiency. The optimal parameters of the probability distribution are found by reducing the distance between two sampling distributions, which is measured by Cross Entropy (CE). Strong globally search capabilities, excellent flexibility, and great resilience are features of the CE approach.

$$CE = \frac{1}{N}\sum_{i=1}^{N} I_{s<r} \frac{f(x^i,v)}{g(x^i)} \quad (6)$$

where x^i is a random sample from f(x;v) and g(x) is the sampling density of significance. To ascertain the optimal importance sampling density, the distance between two sampling distributions is referred to as the Kullback–Leibler divergence, or cross-entropy.

Algorithm 1 illustrates the general procedures used in the suggested EBO algorithm. Step 1 of Algorithm 1 generates the initial population by counting the number of nodes in the IoT-based WSN. Step 2 computes the stimulus intensity I_i at x_i based on the sensor modality c and power exponent a. The reduced energy use is the source of these variables. Following that, the stopping conditions are determined (Step 4), and the fragrance value is calculated (Step 6) for every butterfly in the network. Then, in Step 8, determine which node in the population is the best, and in Step 10, produce a random number, r. Proceed to the best butterfly using equation (11), if r<p; if not, proceed at random using equation (12). Following that, update a value (Step 17) and assess people based on their new positions (Step 18). Finally, use end while (Step 19) to terminate the process. Figure 3 shows the suggested EBO algorithm's flowchart.

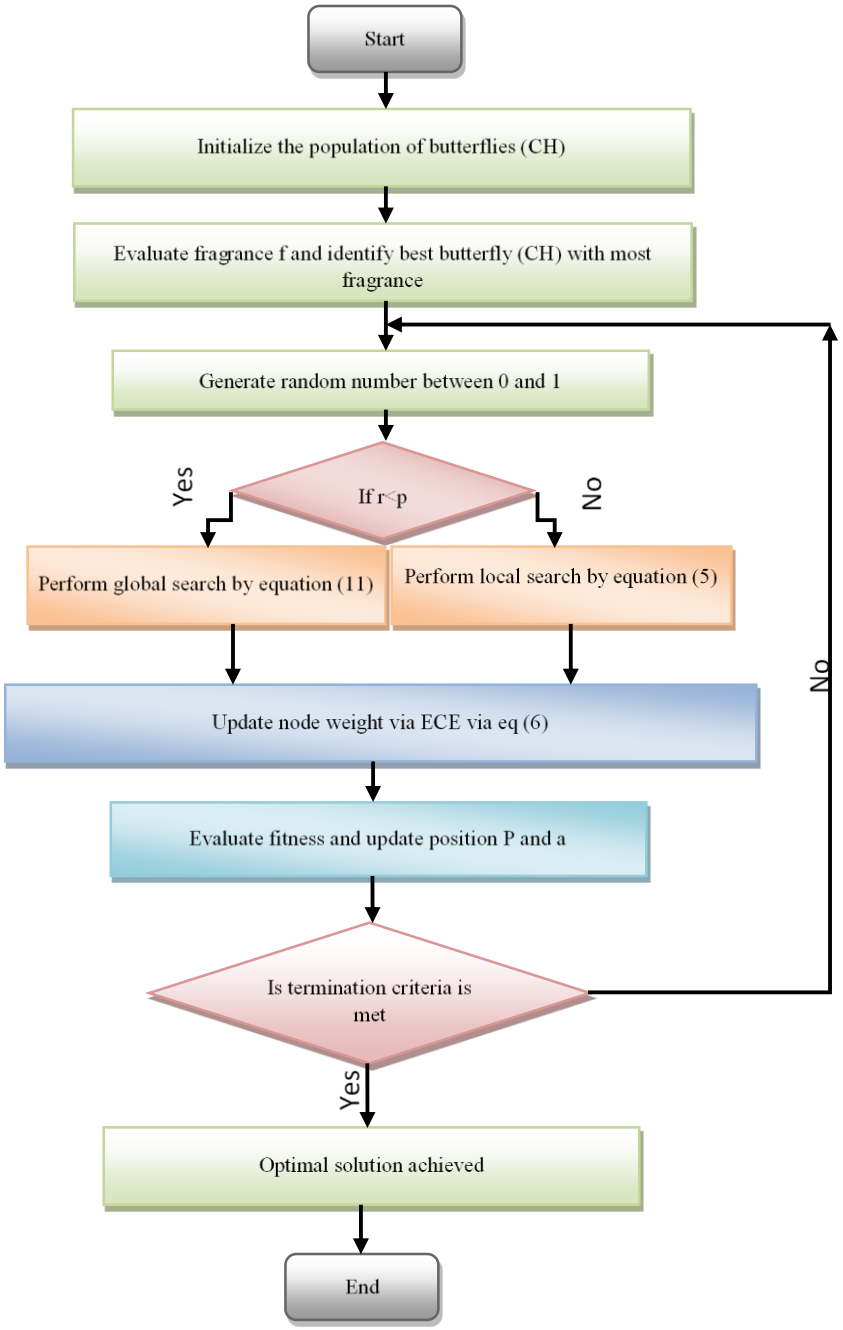

Fig 3 Flowchart of Entropy Butterfly Optimization Algorithm (EBO)

Algorithm 1: EBO algorithm for optimal CH node selection

1. Create the initial n butterfly population, $x_i = (i = 1,2, \dots, n)$
2. Reduced energy consumption $f(x_i)$ indicates the stimulus intensity I_i at x_i.
3. Define sensor modality c, power exponent a and switch probability p
4. While stopping criteria not met do
5. For each butterfly f in population do
6. Calculate fragrance for f using equation (5) and generate weight via entropy by equation (6)
7. End for

8. Find the best butterfly
9. For each butterfly f in population do
10. Generate random number r
11. If $r < p$ then
12. Equation (4) will lead you to the best butterfly (optimal CH nodes via reduced energy usage), while equation (6) will provide weight via entropy.
13. Else
14. Move randomly using the equation (5)
15. End if
16. End for
17. Update the value of a
18. Evaluate individuals(CH) according to their new position

3.3 Shortest path routing and spoofing attack detection using Improved Dynamic Source Routing (IDSR) protocol in MANET

In this work, shortest path routing and spoofing attack detection is done by using IDSR protocol over MANET. The network performance has been enhanced through trust and optimal route selection. In this study, available and optimal routes are generated sequentially using the proposed model. When a source transmits a packet to its destination, the routing route is decided by the on-demand source routing protocol known as DSR (Dynamic Source Routing). Multi-hop ad hoc networks of mobile nodes are optimal for DSR's reactive routing protocol, enabling the networks to completely self-organize and self-configure without any centralized infrastructure. To identify connection failures and prevent route loops, DSR makes use of the MAC layer. To enable nodes to recognize and maintain source routes to destination nodes, it performs two key functions: route discovery and route maintenance.

To establish a route, the source node broadcasts Route Request (RREQ) packets to each node in the MANET. The nodes that receive the RREQ packets utilize the route cache to determine their position with respect to the designated destination nodes. Route Reply (RREP) packets are sent back by the nodes if they are closer the destination; if not, the RREQ packets are discarded. The source node decides whether to add an intermediate node to the route after examining the packet header for the UID when it receives RREP packets from those nodes. Routes are developed in this manner. The DSR route discover procedure is shown in Figure 4.

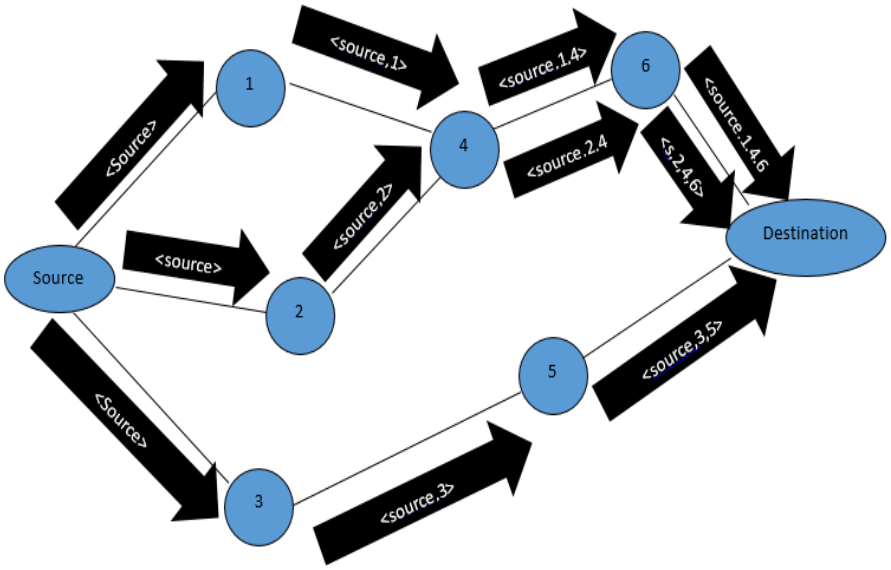

Fig 4 Route discovery phase

Functional routes are maintained and connection failures are fixed during the route maintenance phase. In Figure 5, the DSR route maintenance procedure is shown. A packet-forwarding node above of its adjacent node's broadcast range results in a connection failure. Packet transmission terminates as a consequence, and the nodes notify the source node of the Route Error (RERR). When this happens, the source retransmits the packet using several routes and isolates the unsuccessful route. While forwarding a packet, an upstream node notifies the source node of a link failure by sending it an RERR message. Initiating a new route discovery process, the source node identifies other routes while the MAC layer examines the condition of the node that is causing the connection failure. In Algorithm 2, the IDSR process is shown.

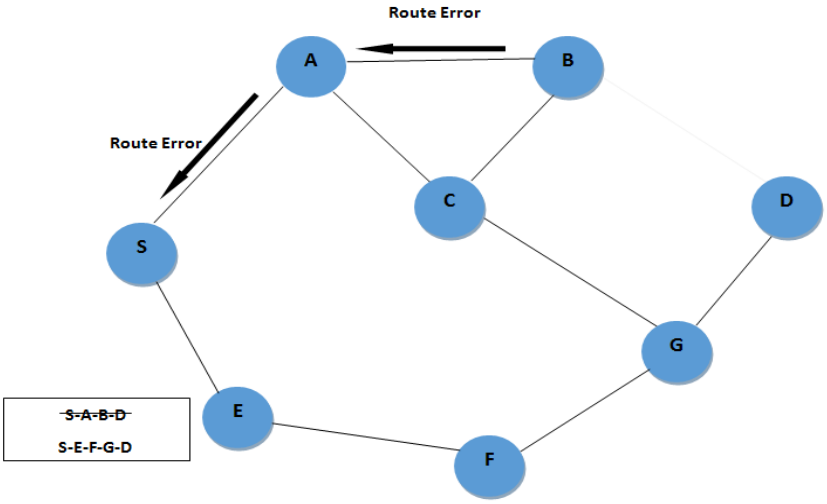

Fig 5 Route maintenance phase

In this protocol, each node regularly assesses its neighbors' level of trust, maintaining a separate trust value for each one. The trust level is determined by observing and monitoring the behavior of the neighbor. This trust value helps decide whether a neighbor is considered trustworthy or potentially malicious. A node will be eliminated before the route is created if its trust level falls below a certain level, signaling that it is malicious. The routing mechanism will not include nodes with low trust levels.

Transmitting communication packets exclusively to trustworthy neighbor nodes, a trust mechanism improves IDSR. Trust is computed using each node's activity and behavior data, which are divided into two categories: TL (Trust Local) and TG (Trust Global). TG stands for the trust computation, which is based on the total number of routing packets sent and received. By utilizing TL, a neighbor node compares the total number of packets received and the number of packets broadcast from certain nodes. Nodes use the sum of the TL and TG values to calculate the total trust level of their neighbors.

Algorithm 2: IDSR protocol for spoofing attack detection and shortest path routing

Initialize N mobile nodes

if i node is source node

Create RREQ packets

With source, destination, unique, path, RERR, and timer t, broadcast an RREQ packet

Establish the shortest path route using route discovery and maintenance process

Compute trust values using TG and TL nodes

If the path in the routing database is valid, begin the data transmission

Receive RREP packets

Check node UID

Start the route discovery

Detect early spoofing attack

If Particular node is S, I and F node

Assign the particular node as spoofing node

Then

Discard the S, I and F node

If Particular node is E node

Assign the particular node as spoofing node

Then

Remove the spoofing attack from the node

Return the node as R node

Perform minimum distance for packet transmission

Return all possible shortest paths

Select best short routing paths

Continue to data transfer

Stop

Analyze the received data packets using the data count that was provided by the sender

As PD, calculate the probability that packets will reach the desired node

The procedure of starting RREP

If $P_D<T_{EL,\ PL}$ (where $T_{EL,\ PL}$ is the network's threshold for energy loss and packet loss)

Provide the source node with a positive acknowledgment (ACK)

Else

Lower packet loss and start the node with the optimum energy usage

Repeat the trust condition

End if

Algorithm 2 outlined above focuses on selecting the shortest routing path using optimal parameters. The protocol supports on-demand route discovery and maintenance, incorporating node sequence numbers to adapt to changes in topology and routing information. Spoofing attack detection is performed efficiently, improving the MANET's data transfer security. Utilizing the shortest route, least distance, and energy usage to share many bits of information, it guarantees secure data transfer. A cloud server receives data from the IoT-based WSN, which has several sensors, over the internet. Additionally, internet services are used by the MANET to send, receive, and store data. For data transmission or reception between the MANET and cloud systems via gateways, this creates a heterogeneous network. Connecting the MANET to the cloud occurs through the gateway nodes.

4. SIMULATION RESULT

The simulation is conducted using ns-2. Mobile MANET nodes and cloud network (WSN) nodes connected to the Internet are used to form the environment. Small clusters of mobile ad-hoc nodes organize the sensor nodes. Based on their energy levels, nodes designated as Cluster Heads (CH) are in charge of managing the sensor nodes. To determine the routes from the sensor source to the gateway node, they make use of the MANET cluster and an on-demand routing protocol. By determining the route's total energy, the time it takes to get there, and the number of hops, the best route is identified. By considering node energy levels into account, this method guarantees consistent IoT connectivity for extended stretches of time. Furthermore, for the chosen routes among the trust validation technique enhances the latency, throughput, energy efficiency, and packet delivery ratio of the clusters. The implementation makes use of the suggested EBO-IDSR protocols, ESO [15], and the already-existing BOA-ACO [13]. Table 1 lists the hybrid network's simulation parameters.

Table 1: Simulation parameters

Parameter	values
No. of sensor nodes	100
No. of mobile nodes	500
Area Size	1100 * 1100(Meter)

Mac	802.11
Total energy	150 Joule
IoT Frequency Band	2.4–5 GHz
Initial value of energy	1.5 Joule
Radio Range	250m
Routing protocol	DSR
Simulation Time	60 sec
Packet Size	500–1500 bits

4.1 Energy consumption

The average energy used to send, receive, or forward a packet to a network node during a certain time period is referred to as energy consumption.

$$Energy\ (e) = [(2 * pi - 1)(e_t + e_r)d \quad (7)$$

The data packet pi, the transmission energy e_t, and the reception energy e_r, and d is the distance between the transmission and destination nodes.

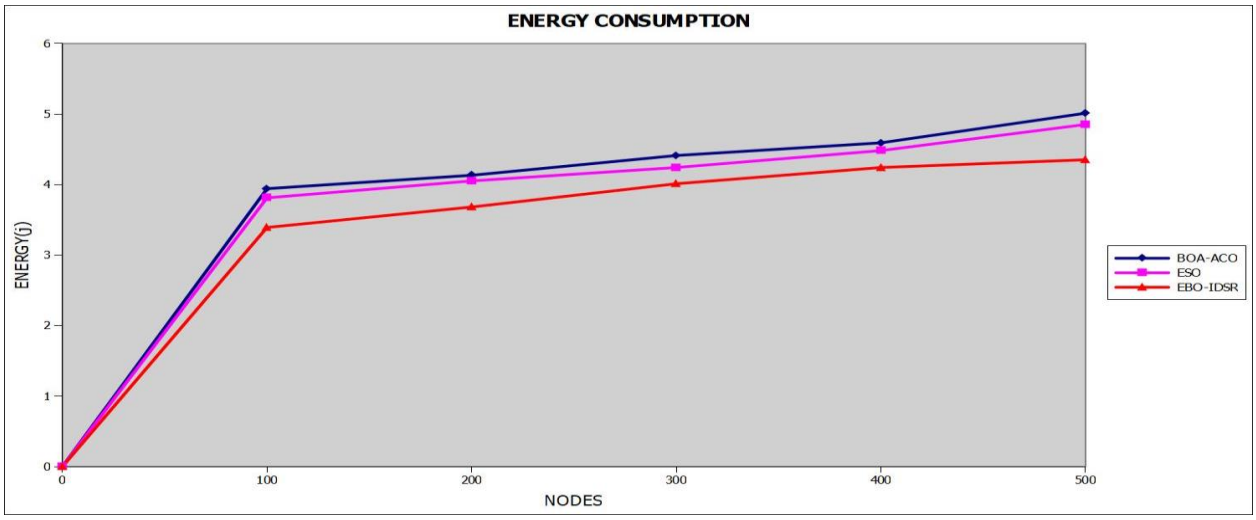

Fig 6 Energy consumption comparison

Figure 6 compares EBO-IDSR, BOA-ACO, and ESO energy utilization. The number of nodes is on the x-axis, while energy is on the y. The suggested EBO algorithm dramatically lowers the hybrid network's overall energy usage during data packet transmission. Through a trust mechanism, the IDSR protocol improves dependability while concentrating on route routing optimization. The results demonstrate that the existing methods consume more energy, whereas the proposed BOA-ACO and ESO algorithms achieve lower energy consumption.

4.2 Throughput:

The rate of successful data packet transmission using a network or communication connection is known as throughput.

$$Throughput = total\ number\ of\ packets\ sent\ /time \quad (8)$$

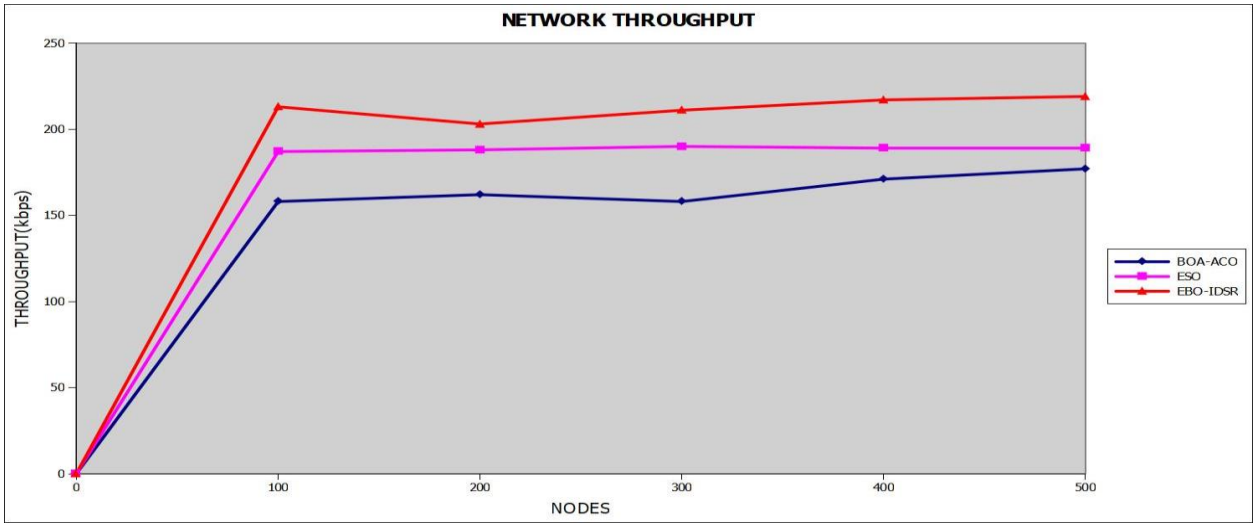

Fig 7 Throughput comparison

Fig 7 illustrates the comparison between the existing BOA-ACO, ESO and proposed EBO-IDSR algorithms for the throughput metric. Throughput is measured on the y-axis, while the number of nodes is measured on the x-axis. The proposed IDSR protocol is used to determine the spoofing attacks using route discovery and maintenance criteria effectively in MANET. EBO algorithm is used to select best CH nodes by generating best fitness via lower energy consumption. As a result, a heterogeneous network is established to facilitate data transfer or reception between the MANET and cloud systems over the internet. The comparison shows that the existing BOA-ACO and ESO methods yield lower throughput, while the proposed EBO-IDSR algorithm achieves higher throughput.

4.3 Packet Delivery Ratio (PDR)

The number of packets that the destination successfully receives is known as the packet delivery ratio.

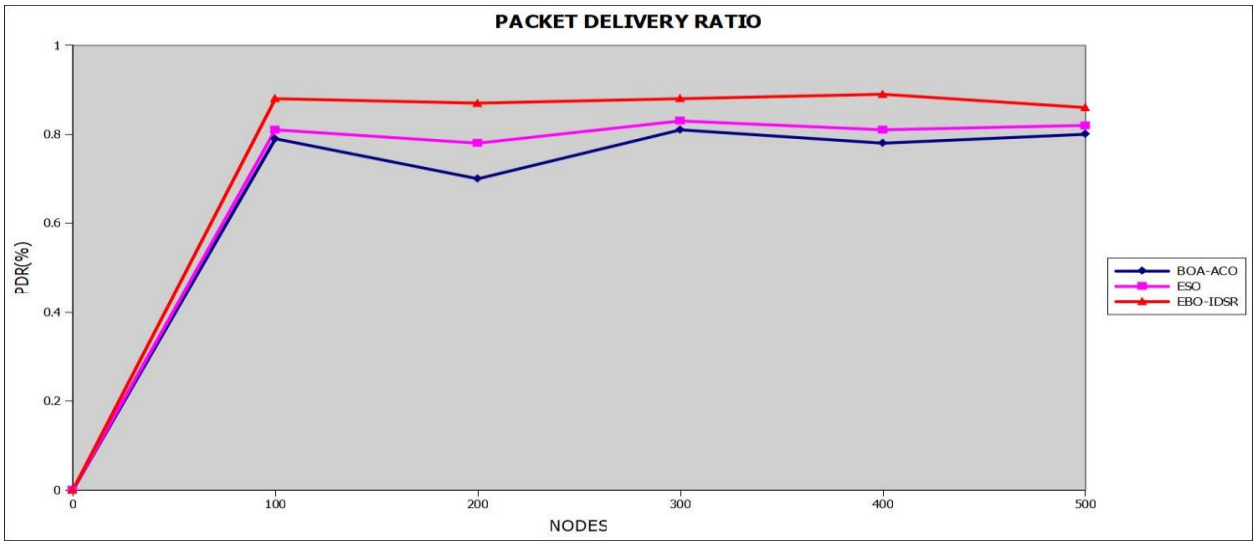

Fig 8 Packet delivery ratio

As shown in Figure 8, a comparison is made between the existing BOA-ACO, ESO, and the proposed EBO-IDSR protocol in terms of PDR. While the x-axis shows the number of nodes, the y-axis shows the PDR values. In the existing scenario, the PDR values are lower when using the BOA-ACO and ESO methods. However, with the proposed system, the PDR value significantly improves using the EBO-IDSR protocol. Additionally, using internet services, the MANET sends, receives, and saves data. This illustrates how the suggested trust-based IDSR protocol may transmit data in a hybrid network with efficiency and security.

End-to-end delay

The end-to-end delay is the average time required for a packet to get from its source to its destination throughout a network.

$$End - to - end\ delay = \frac{\sum_{i=1}^{n}(t_{ri} - t_{si})}{n} \quad (9)$$

Where n is the total number of packets, t_{ri} and t_{si} are the receive and send times, respectively, of the i-th packet.

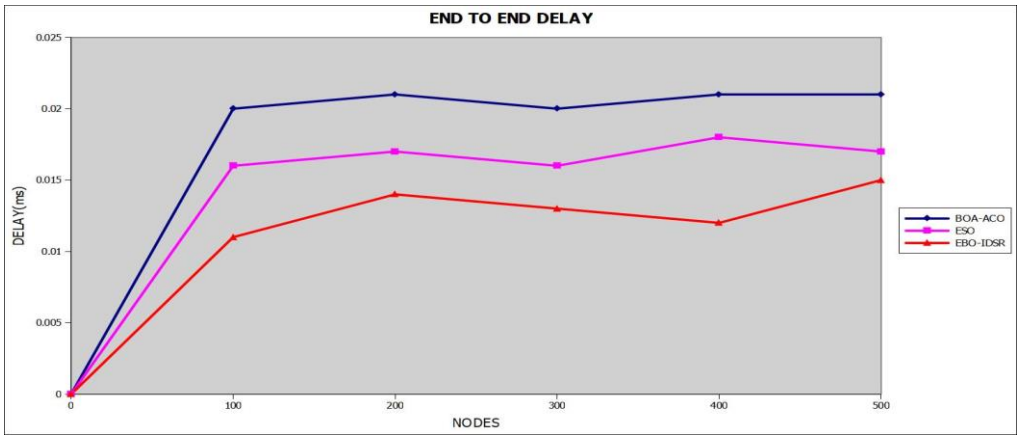

Fig 9 End-to-end delay comparison

The end-to-end delay performance of the suggested EBO-IDSR protocol, the existing BOA-ACO, and ESO is contrasted in Figure 9. The y-axis shows the end-to-end delay metric, while the x-axis plots the number of nodes. During secure data transmission, the proposed EBO-IDSR protocol significantly reduces the transmission time across the WSN. The IDSR protocol enhances the efficiency and reliability of path routing in MANET with IoT, specifically for detecting spoofing attacks. In comparison to the existing BOA-ACO and ESO algorithms, the results of the simulation demonstrate that the proposed EBO-IDSR protocol reduces the end-to-end latency.

Overhead

The proposed algorithm should provide lower overhead

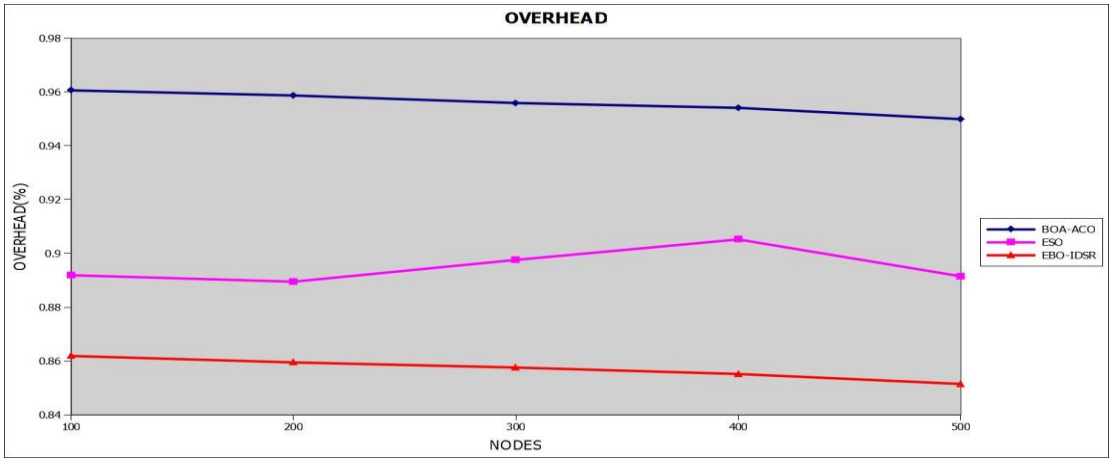

Fig 10 Overhead

Fig 9 illustrates the comparison between the existing BOA-ACO, ESO and proposed EBO-IDSR protocol for the overhead. There are nodes on the x-axis, and the end-to-end latency metric is on the y-axis. The proposed EBO-IDSR protocol provides lower overhead in MANET with IoT for finding spoofing attacks. The simulation result shows that the proposed EBO-IDSR protocol yields a lesser overhead than the existing BOA-ACO and ESO algorithms

5. CONCLUSION

In this study, the EBO-IDSR protocol is applied to optimize the selection of Cluster Head (CH) nodes and ensure secure data transmission across the hybrid network. Based on fitness values, the EBO method is presented for selecting the optimal CH node. To identify the most efficient CH node selection option, its fitness function takes into account variables including end-to-end delay, throughput, and remaining energy. The IDSR protocol focuses on enhancing secure shortest-path routing through route discovery and maintenance, thereby improving the performance of the hybrid network. The EBO-IDSR

protocol helps prevent spoofing attack nodes, significantly reducing packet loss. Connecting the MANET to the cloud is done via the gateway nodes. In terms of throughput, packet delivery ratio, and network lifetime, the findings demonstrate that the proposed EBO-IDSR protocol performs more than existing BOA-ACO and ESO algorithms. It also uses reduced energy. Future work may involve the development of hybrid swarm optimization and new encryption algorithms to address computational complexity challenges more effectively.

REFERENCES

[1] Srilakshmi, U., Alghamdi, S. A., Vuyyuru, V. A., Veeraiah, N., & Alotaibi, Y. (2022). A secure optimization routing algorithm for mobile ad hoc networks. *IEEE Access*, *10*, 14260-14269.

[2] Tripathy, Bata Krishna, et al. "An adaptive secure and efficient routing protocol for mobile ad hoc networks." *Wireless Personal Communications* 114.2 (2020): 1339-1370.

[3] Bhardwaj, Antra, and Hosam El-Ocla. "Multipath routing protocol using genetic algorithm in mobile ad hoc networks." *IEEE Access* 8 (2020): 177534-177548.

[4] Tilwari, Valmik, et al. "MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks." *Wireless Personal Communications* 112 (2020): 2461-2483.

[5] Shukla, Anurag, and Sarsij Tripathi. "An effective relay node selection technique for energy efficient WSN-assisted IoT." *Wireless Personal Communications* 112.4 (2020): 2611-2641.

[6] Baradaran, Amir Abbas, and Keivan Navi. "HQCA-WSN: High-quality clustering algorithm and optimal cluster head selection using fuzzy logic in wireless sensor networks." *Fuzzy Sets and Systems* 389 (2020): 114-144.

[7] Alghamdi, Turki Ali. "Energy efficient protocol in wireless sensor network: optimized cluster head selection model." *Telecommunication Systems* 74.3 (2020): 331-345.

[8] Singh, Priyanka, Manju Khari, and S. Vimal. "EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT." *Wireless Personal Communications* 126.3 (2022): 2149-2173.

[9] Hassan, Saad M., et al. "Enhancing MANET Security Through Federated Learning and Multiobjective Optimization: A Trust-aware Routing Framework." *IEEE Access* (2024).

[10] Hussein, Safwan Mawlood, Juan Antonio López Ramos, and Abubakar Muhammad Ashir. "A secure and efficient method to protect communications and energy consumption in IoT wireless sensor networks." *Electronics* 11.17 (2022): 2721.

[11] Narendran, M., and Periyasamy Prakasam. "An energy aware competition based clustering for cluster head selection in wireless sensor network with mobility." *Cluster Computing* 22.Suppl 5 (2019): 11019-11028.

[12] Aroulanandam, Vijay Vasanth, et al. "Improving the Energy Efficiency in Mobile Ad-Hoc Network Using Learning-Based Routing." *Revue d'Intelligence Artificielle* 34.3 (2020).

[13] Maheshwari, Prachi, Ajay K. Sharma, and Karan Verma. "Energy efficient cluster based routing protocol for WSN using butterfly optimization algorithm and ant colony optimization." *Ad Hoc Networks* 110 (2021): 102317.

[14] Benakappa, S. M., and M. Kiran. "Energy aware stable multipath disjoint routing based on accumulated trust value in MANETs." *International Journal of Computer Network and Information Security* 14.4 (2022): 14.

[15] Krishnamoorthy, Vinoth Kumar, et al. "Energy saving optimization technique-based routing protocol in Mobile ad-hoc network with IOT Environment." *Energies* 16.3 (2023): 1385.

[16] Daniel, Jesline, Sangeetha Francelin Vinnarasi Francis, and S. Velliangiri. "Cluster head selection in wireless sensor network using tunicate swarm butterfly optimization algorithm." *Wireless Networks* 27 (2021): 5245-5262.

[17] Pratha, S. Jaya, Valayapathy Asanambigai, and Seenapuram Rajan Mugunthan. "Hybrid Mutualism Mechanism-Inspired Butterfly and Flower Pollination Optimization Algorithm for Lifetime Improving Energy-Efficient Cluster Head Selection in WSNs." *Wireless Personal Communications* 128.3 (2023): 1567-1601.

[18] Ghaleb, Sulaiman Abdo Mahyoub, and V. Vasanthi. "Energy efficient multipath routing using multi-objective grey wolf optimizer based dynamic source routing algorithm for manet." *Int J Adv Sci Technol* 29.3 (2020): 6096-6117.