International Journal of Advanced Trends in Engineering and Management
(ISSN 2583-7052)

Vol. IV, No. 06, pp. 22-32, June

Modified Fuzzy Based Cluster Head Selection and Pity Beetle Optimization-Based Secure Routing for MANET

Balaji V[1], Samuel Isaac Tecle[2], E. Maheswari[3]

[1]Department of Electrical and Electronics Engineering, MAI-NEFHI College of Engineering, Asmara, Eritrea.
balajieee79@gmail.com
[2]Head of the Department, Department of Electrical and Electronics Engineering, MAI-NEFHI College of Engineering,
samuel47tecle@gmail.com
[3]Associate professor, Department of Electrical and Electronics Engineering, Sri Sairam Institute of Technology, Chennai.
maheswarieee@gmail.com

***Corresponding Author E-mail:** balajieee79@gmail.com

ABSTRACT: Mobile Ad Hoc Networks (MANETs) are dynamic, infrastructure-less networks that rely on node cooperation for communication throughout the environment. It is a collection of autonomous, self-organizing mobile nodes that are connected without the need for a centralized infrastructure. Efficient clustering and secure routing are essential for improving the performance, stability, and security of such networks. This paper proposes a hybrid approach that combines Modified Fuzzy-Based Cluster Head (CH) Selection with Pity Beetle Optimization (PBO) for secure routing, and integrates Philippine Eagle Optimization (PEO) for global route enhancement. The fuzzy-based method ensures optimal and energy-efficient selection of CHs, while PBO strengthens route security against potential intrusions. PEO further refines the path selection, enhancing data delivery and minimizing latency. Experimental results demonstrate that PBO-PEO significantly reduces energy consumption, enhances packet delivery, and prolongs network lifetime, outperforming traditional routing protocols. The proposed framework contributes to the development of intelligent, power-aware routing protocols for MANETs, ensuring sustainable and resilient network communication. The suggested PBO-PEO have a longer network lifetime of 2400, higher throughput of 5ms, better energy consumption of 990, and less delay 12ms.

Keywords: Mobile Ad Hoc Networks, Fuzzy clustering, Pity Beetle Optimization, Philippine Eagle Optimization, Cluster Head

1. Introduction

In MANET all node is equipped with a radio transmitter as well as a receiver, enabling wireless bidirectional communication with the system [1]. Due to their self-configuring and infrastructure-less characteristics, MANETs have attracted a lot of interest. Consequently, MANETs are essential for a variety of applications, including disaster recovery, military communications, and mobile sensing [2]. MANETs are made up of mobile nodes that connect to one another via a wireless link, as opposed to traditional networks, which are dependent on fixed infrastructure [3]. Whereas, a rapid deployment and reconfiguration are possible by this flexibility, which is especially helpful in situations where traditional network infrastructure is either unfeasible or unavailable [4]. However, one of the main issues with MANETs is the variability in the trustworthiness of network nodes because the dynamic topology and lack of centralized control make malicious behaviour difficult to detect and mitigate [5-6]. Conversely, the features that make MANETs appealing also present significant challenges, particularly with regard to ensuring secure and reliable communication [7]. Moreover, for a MANET to work properly, its nodes must cooperate, but this dependence on cooperation also leaves the network vulnerable to a number of security risks, including gray hole attacks, in which nodes selectively drop packets, and black hole attacks, in which malicious nodes advertise false routes to intercept and discard packets [8]. Figure 1 shows the MANETs structure. To address this challenge some of the following optimization techniques are utilized in secure routing for MANETs.

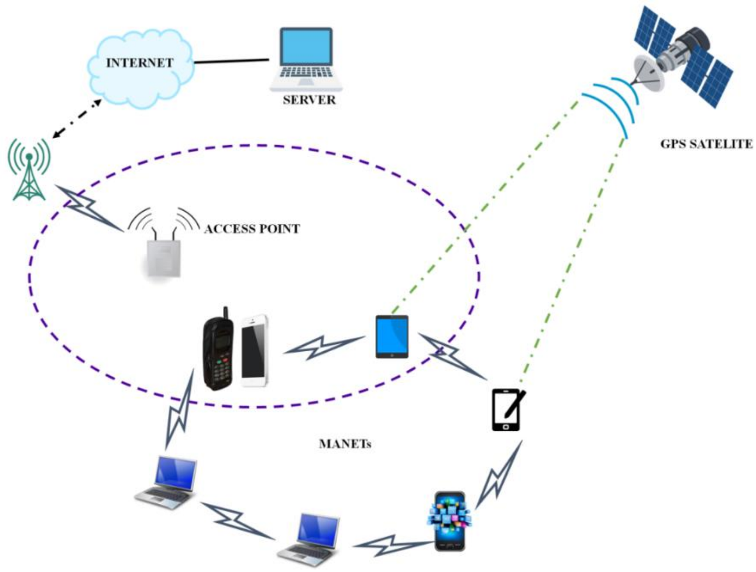

Figure 1: *MANETs structure*

To optimize the secure routing some of the following existing methods are utilized for MANET. In order to secure the routing for MANET Location-Aided Routing (LAR) with Optimized Particle Swarm Optimization (OPSO-LAR) is utilized. The computing function's parameter is optimized using the PSO approach. Additionally, it is utilized to select between two or more node coverage and network flooding variables. Nevertheless, OPSO-LAR are quick converge to local optima, especially in complex or high-dimensional search spaces like MANETs with dynamic topologies [9]. Consequently, Genetic Algorithm with Hill climbing (GAHC) picks the optimal route in multipath. The combination of GA for global exploration and HC for local exploitation ensures better quality routes, balancing optimality and security. Hill climbing improves solutions quickly after crossover and mutation, serving GAHC converge faster in dynamic MANETs. Nonetheless, if improperly tuned, HC algorithm gets stuck in local optima, particularly in sparse or highly mobile networks [[10]. Additionally, to establish multiple paths between the source and destination nodes in a MANET by developing a hybrid routing protocol that integrates the strengths of AODV (Ad hoc On-Demand Distance Vector) and MBOMRP (Multi-Path Byzantine Optimized Link State Routing Protocol)Broken links is detected and repaired dynamically using Route Error (RERR) messages, supporting reliable data delivery. However, AODV realises and maintains only one path at a time, making it less resilient to attacks [11].

For MANET the optimized routes are secured using the Adaptive Cuckoo Search Optimization (ACSO). After that, an entropy-based signature is applied to each node in the cluster. The node's future position is then ascertained by estimating the link lifetime and travel distance. ACSO avoids local optima by performing a diversified global search, improving the chances of finding optimal and secure routes in a dynamic MANET. Nevertheless, ACSO struggle to converge quickly in environments with rapid topology changes, potentially delaying secure route establishment [12]. Whereas, a Coot Chimp Optimization Algorithm- Deep Q-Network (CChOA-DQN) for detecting the black hole attacks in MANET. CChOA integrates the exploration strength of coots and the exploitation power of chimps, preventing premature convergence and ensuring optimal secure path discovery. Nonetheless, the continuous learning and optimization process increase energy usage, reducing node lifespan if unoptimized properly [13].

Additionally, to improve the energy efficiency of the MANET network Hybrid Swallow Swarm Optimisation-Memetic Algorithm (SSO-MA) is utilized. SSO handles global search, whereas the mimetic component performs local improvements, ensuring efficient and high-quality routing decisions. Nonetheless, designing and tuning both the global SSO and local MA components requires careful parameter selection and complex system architecture [14]. Moreover, Modified Whale Optimization Algorithm (MWOA) is used to provide a secure clustering and routing solution in MANET. By optimizing routes based on residual energy, MWOA helps prolong network lifetime by avoiding overused or energy-depleted nodes. However, MWOA increase computational complexity, creating it less suitable for low-resource or lightweight MANET nodes [15]. To overcome the limitation of secure routing from source to destination the proposed PBO integrates PEO is utilized for MANETs.

2. Related work

Veeraiah *et al* [16] (2021) have suggested a Hybrid algorithm called the Cat Slap Single-Player Algorithm (C-SSA) for secure and energy-efficient routing in MANETs. C-SSA is to identify high-value nodes that contribute positively to network stability and security. C-SSA protocol selects optimal paths by analysing key performance metrics such as latency, connectivity, and throughput, with a particular emphasis on maximizing data throughput rather than simply minimizing energy or delay. However, to process multiple trust metrics and performance parameters, C-SSA have delay route formation, creating it less suitable for time-sensitive applications.

Veeraiah *et al* [17] (2022) have presented a Bird Swarm-Whale Optimization Algorithm (BSWOA) method is utilized to improve multipath routing in MANETs. BSWOA ensures a global search for optimal routes (BSA) and refined local search for route stability (WOA), reducing the risk of local optima and improving routing efficiency. BSWOA reacts to changes in node mobility, topology, and link quality for MANET routing. Nevertheless, in very large MANETs, the complexity of maintaining and updating candidate solutions (routes) lead to scalability issues and increased overhead.

Srilakshmi *et al* [18] (2022) have developed a Bacteria for Aging Optimization Algorithm (BFOA), to finds the ideal hops in advancing the routing. BFOA is utilized to offer a trust-based protected and energy-efficient navigation in MANETs. The elimination-dispersal step allows BFOA to handle frequent mobility or node failure, creating it highly adaptable to MANETs. Yet, due to its iterative nature, BFOA is slower, especially during route discovery. Performance depends on parameters like step size, chemotactic steps, which is hard to fine-tune in real-time.

Ravi *et al* [19] (2023) have proposed a Fuzzy Butterfly Optimization Algorithm (FBOA) and Adaptive Chaotic Grey Wolf Optimization (ACGWO) algorithm provides secure communication in MANETs. FBOA-ACGWO incorporates fuzzy trust models to evaluate nodes, avoiding malicious or unreliable nodes, thus enhancing security. ACGWO is capable of optimizing for delay, packet delivery ratio, trust, and energy simultaneously. Nonetheless, the combination of adaptive controls and chaotic maps makes the algorithm difficult to design and tune properly.

Arulselvan G and A. Rajaram [20] (2025) have presented a Dolphins Echolocation then the Cat Swarm Optimization algorithms, to secure the routing in the MANETs. Dolphin Cat Optimizer determines the optimal path allowing to the modelled unbiased function that considers trust factors, such as present trust, past trust, together direct as well as indirect trust, delay, distance, in addition to linking lifespan. Dolphins Echolocation is an iterative search process to changing topologies and node mobility, creating it well-suited for MANETs. However, performance relies on properly tuned parameters like seeking memory pool size and mixture ratio, which is difficult in MANETs.

The contribution of the work

- Developed a Modified Fuzzy-Based Cluster Head Selection system that improves energy efficiency and extends network lifetime.
- Integrated PBO to enhance routing security by avoiding malicious or untrusted nodes for further optimization.
- Applied Philippine Eagle Optimization (PEO) for optimal route refinement, reducing end-to-end delay and improving path reliability.

3. Proposed work

The proposed work in figure 2 shows a novel hybrid routing framework for MANETs that integrates Modified Fuzzy-Based CH Selection, PBO, and PEO to address the challenges of secure, efficient, and reliable communication in dynamic, infrastructure-less environments. Initially, the fuzzy logic-based clustering mechanism evaluates parameters such as residual energy, node degree, and trust level to identify the most suitable and energy-efficient nodes as cluster heads, thereby enhancing network stability and lifetime. Once clusters are formed, the PBO algorithm is employed for secure intra-cluster and inter-cluster routing, mitigating threats by prioritizing routes through trustworthy and less vulnerable nodes.

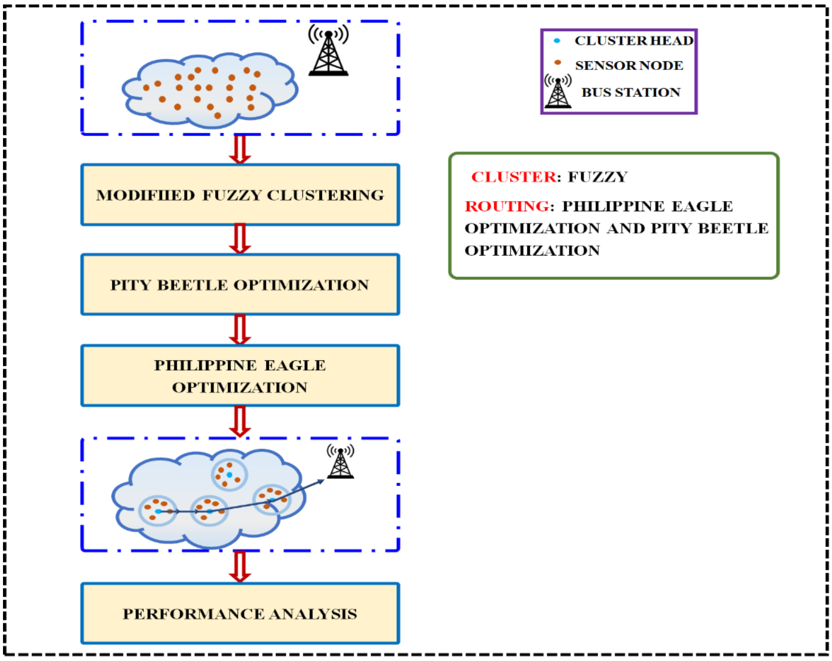

Figure 2: *Block diagram of the proposed work*

To further optimize routing performance at global level, PEO is applied to refine route paths by considering key metrics such as connectivity, throughput, and latency, ensuring robust and timely data transmission. This integrated approach effectively balances security and energy efficiency, MANET routing protocols are evaluated based on key performance metrics such as packet delivery ratio, energy consumption, and resilience against security attacks

3.1 Fuzzy-Based Cluster Head Selection approach in MANETs

The Modified Fuzzy-Based CH Selection approach in MANETs is to improve the stability and efficiency of the network by intelligently choosing CHs based on multiple parameters such as residual energy, trust value, mobility, and node degree. However, if not properly designed or calibrated, this method become vulnerable to insecure node selection. Specifically, the fuzzy logic system depends on the accuracy of input metrics like trust levels. In dynamic environments, malicious nodes manipulate trust metrics, causing the algorithm to misidentify them as reliable CHs. Figure 3 shows the flow chart for the fuzzy clustering in MANETs.

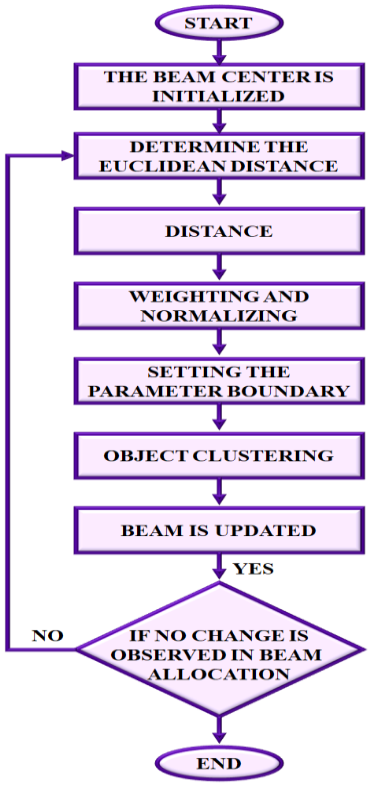

Figure 3: *Flow chart for fuzzy clustering Generation of Cluster in MANET*

The positions of Cluster Supporters are represented by $N = \{n_1, n_2, \dots, n_m\}$ in MANET then these Cluster Members (CM) are clustered into l set $L = \{l_1, l_2, \dots l_i\}$. Equation show the fuzzy clustering in MANETs.

$$G(N, D, S) = \sum_{s=1}^{i} \sum_{q=1}^{m} d_{sq} \left\| n_q - \gamma_s \right\|^2 \qquad (1)$$

Wherever the speed among nodes (CM) are denoted by $S(\gamma_s; s = 1, \dots i)$ and the distance between nodes are denoted by $D\left(d_{sq}; s = 1, \dots . i, q = 1, \dots . m\right)$. The q^{th} membership degree to the s^{th} cluster is described in equation

$$\gamma_s = \frac{\sum_{q=1}^{h} d_{sq} n_q}{\sum_{q=1}^{h} d_{sq}} \qquad (2)$$

Where, α denotes the degree value of every node. Effective Clustering is formed by minimizing the value of d_{sq} , besides following three requirements must be met by reduction method.

a) A membership degree ranging from zero to one is awarded to the CM within the MANET.

$$d_{sp} \in [0,1], \; s = 1, \dots . i, \; q = 1, \dots . . h. \qquad (3)$$

b) For a single CM, the sum of all membership degrees must equal one.

$$\sum_{s=1}^{i} d_{sp} = 1, \quad q = 1, \ldots\ldots h \tag{4}$$

c) A minimum of one Cluster Member with a non-zero membership degree is required.

$$\sum_{s=1}^{i} d_{sp} > 0, \quad s = 1, \ldots\ldots i \tag{5}$$

Once these requirements are met, an equation is used to estimate the cluster centers.

$$d_{sq} = \frac{e^{-\alpha\|n_q-\gamma_s\|^2}}{\sum_{b=1}^{i} e^{-\alpha\|n_q-\gamma_s\|^2}} \tag{6}$$

This leads to potential routing disruptions, packet drops, or information leakage, as CHs are central to data aggregation and route coordination. Therefore, the fuzzy-based CH selection improves efficiency; it must be stimulated with robust trust evaluation and anomaly detection to prevent the selection of insecure or compromised nodes in MANETs.

3.2 Pity Beetle Optimization for secure routing in MANETs

The PBO algorithm is applied to MANETs appeals inspiration from the swarm and duplicate behaviour of beetles in a forest, modelled through three main phases: the search stage (SS), aggregation stage, and anti-aggregation stage. In the SS, nodes act as pioneers, scanning the network to detect communication or trust metrics analogous to chemical traits to identify optimal and secure routes for data transmission. Once a reliable route or node is found, akin to a host tree, the node becomes a central point of attraction, encouraging nearby nodes to converge and forward packets through that path (aggregation stage). This mimics beetles emitting pheromones to attract others to the same location. However, excessive traffic through the same route lead to network congestion, energy depletion, or vulnerability to attacks just as overcrowding causes competition and disease in beetle colonies. To address this, the algorithm enters the anti-aggregation stage, where nodes detect signs of congestion or instability and redirect traffic to alternate secure paths, effectively balancing burden and improving network resilience.

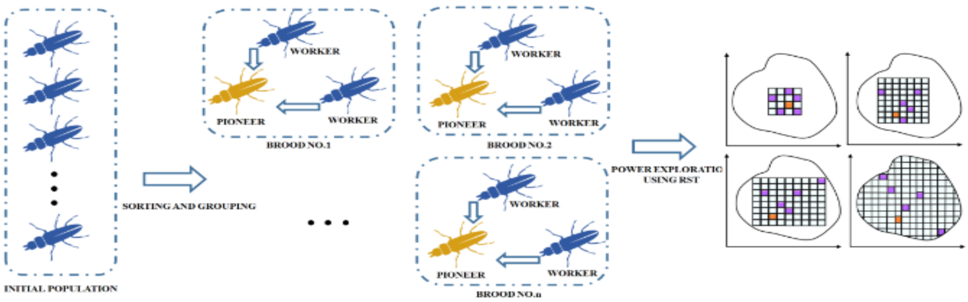

Figure 4: *PBO algorithm for MANETs*

Initialization: PBO Algorithm uses the secure route to generalize the starting population in figure 4.

Searching techniques: Deterministic area search and memory consideration search are the two primary search modes that PBO Algorithm have developed. The population's insects serve as a representation of the decision variable $x \rightarrow$ in Equation (7). Furthermore, the "pioneer" in the current brood is the optimum beetle the choice variable with the lowest fitness value. Utilizing secure routing by the deterministic area search approach creates a random population surrounding the pioneer.

$$[l_t, u_t] \in \left[pioneer_t.\left(1 - f_{pat}\right), pioneer_t.\left(1 + f_{pat}\right)\right], pioneer_t = [x_1, x_2, \ldots x_{Dim}] \tag{7}$$

$$x_{new} = (l_t, u_t, Dim, N_{pop}] \tag{8}$$

Where x_{new} is the new insect produced in the deterministic region and $pioneer_t$ is the optimal choice variable in the current iteration. Figure 5 shows the new beetles that are randomly generated around the pioneer are represented by the purple circle, whereas the orange box is the pioneer as it is at the moment.

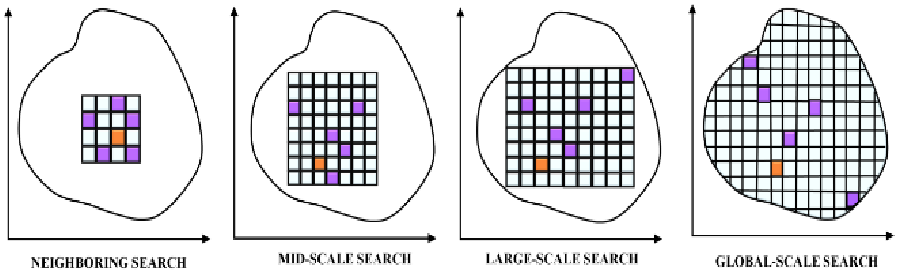

Figure 5: *Searching techniques*

Update strategy: Unlike the conventional biology-based algorithm, PBO Algorithm uses a distinct update strategy. In order to conduct the search operations in the subsequent iteration, the beetles produced in the present iteration are not retained. The remaining beetles in each brood and MEM are eliminated from the population (extinction), leaving only the best beetles (pioneers):

$$x_{t+1} = \begin{cases} pioneer_t \ if \ f(pioneer_t) < f(x_{new} \\ x_{new}, \qquad otherwise \end{cases} \quad (9)$$

Where x_{new} the new choice variable is created in the brood, $f(pioneer_t) \ and \ f(x_{new})$ are the fitness values corresponding to $(pioneer_t), x_{new}$ respectively, and x_{t+1} is the best solution following one iteration. This dynamic behaviour enables PBO to maintain efficient, secure, and adaptive routing in highly mobile and decentralized MANET environments. For global route enhancement PEO technique secure route in MANETs.

3.3 Philippine Eagle Optimization for secure routing in MANETs

The PEO algorithm, inspired by hunting strategy and keen vision of the Philippine eagle, offers a powerful metaheuristic for determining secure and efficient routing paths in MANETs. In this approach, each eagle represents a candidate route, and the goal is to identify the most optimal path based on a fitness function that includes parameters such as trust level (T), residual energy (E), delay (D), and hop count (H).

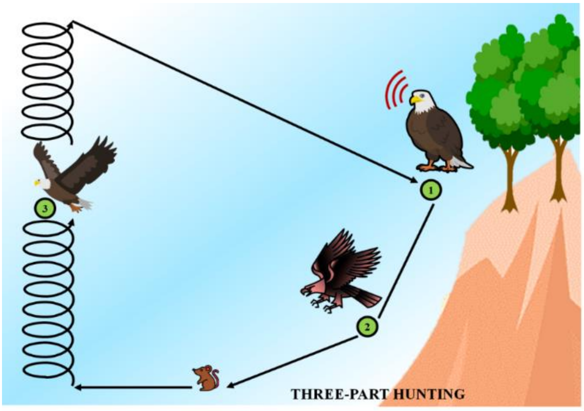

Figure 6: *PEO algorithm*

Figure 6 shows the algorithm mimics the eagle's behaviour in two main phases: exploration, where eagles scan wide areas (search for possible routes), and exploitation, where they dive toward the best prey (select the best path). This behaviour allows the algorithm to balance between global exploration of new paths and local exploitation of promising routes. Figure 7 shows the PEO movement operator in fitness.

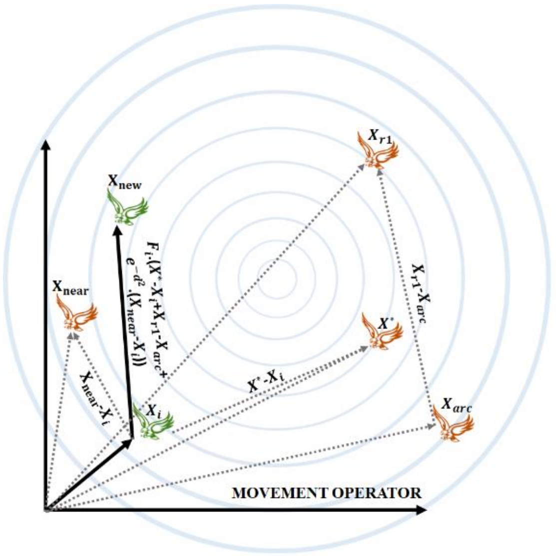

Figure 7: *PEO movement operator for fitness*

The fitness function used for selecting secure routes is defined as:

$$Fitness_i = w_1.T_i + w_2.\frac{E_i}{E_{max}} - w_3.\frac{D_i}{D_{max}} - w_4.\frac{H_i}{H_{max}} \quad (10)$$

Where T_i is trust value of the route, E_i is the residual energy in the route, D_i is the end-to-end delay and E_i is the hop count. w_1, w_2, w_3, w_4 denotes weight coefficients representing the importance of each parameter. By maximizing this fitness function, PEO prioritizes highly trusted and energy-efficient routes whereas minimizing delay and hop count, ensuring secure and stable communication in MANETs. The PEO's ability to adaptively explore and exploit routing options makes it especially effective in dynamic and hostile network environments where traditional protocols struggle with malicious nodes or frequent topology changes.

4. Results and Discussion

The simulation configuration is designed for secure routing using PBO-PEO algorithm in MANETs. This section presents the effectiveness of the future procedure employing PBO-PEO, along with a discussion and comparative analysis

Table 1: *summary of simulation*

Parameters	**Values**
Topology measurement	$500m\ X\ 500m$
Number of nodes	500
First Energy (J) of every node	100 J
Simulation time	100 seconds
Mobility speediness	10 m/s
Border possibility	0.5
Alteration possibility	0.1
Sum of faculty rates	0%
Packet lost rate	0%
Propagation	Open space propagation
Antenna	All-directional

4.1 Experimental Setup

The outcomes for parameters such as throughput, detection rate, delay, and distance are associated with existing system.

4.2 Performance Metrics

The comparison's parameters include the approaches throughput, PDR, energy consumption, network lifetime and delay.

i) Energy consumption

The total power consumption of a system during data packet transmission is called power consumption.

$$E_c = \sum_{i=1}^{N} E_{i,L} \quad (11)$$

Thus, the total energy used by node i following L rounds of data collecting, and N symbolizes the number of nodes.

ii) Throughput

A throughput measurement is expressed in bits per second. The bits transferred to the BS are known as the throughput.

$$T_p = \frac{Received\ packet\ size}{stop\ time - start\ time} \quad (12)$$

iii) Delay

Duration of the sensor node's transmission of the data it has detected from the source to the destination.

iv) Packet Delivery Ratio

PDR is the ratio of all packets transmitted to all packets sent from the origin node.

$$PDR = \frac{packet\ received\ at\ destination}{total\ number\ of\ packet\ send} \times 100 \quad (13)$$

4.3 Comparative analysis

4.3.1 Energy consumption

The energy usage of the suggested PSO-ANN is analysed in the figure 8 using several alternative methodologies. When compared to other current routing techniques the suggested PBO-PEO algorithm provides superior energy consumption performance. The existing methods are BSWOA [17] and BFOA [18] respectively.

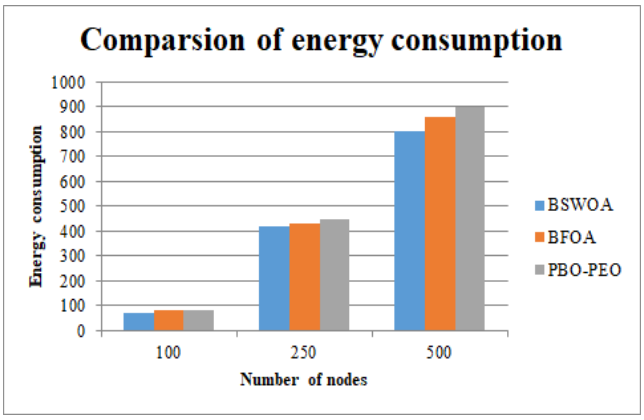

Figure 8: *Comparison of energy consumption*

4.4 Packet Delivery Ratio

The PDR for the proposed structure is displayed in figure 9 in combination that includes BSWOA, BFOA and PBO-PEO. The PDR value for PBO-PEO is high compared to the other technique.

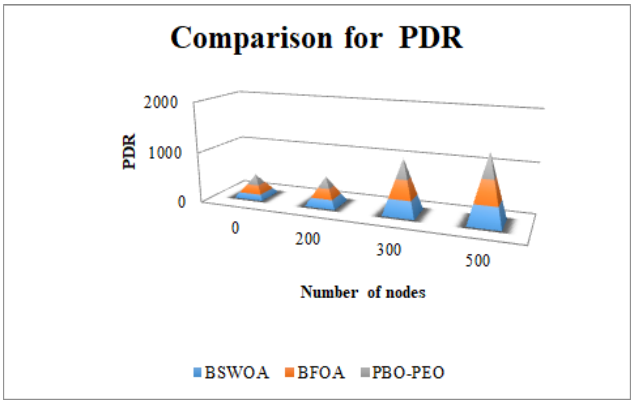

Figure 9: *Comparison of packet delivery ratio*

4.5 Through Put

Figure 10 compares the suggested PBO-PEO throughput analysis with alternative methods. In terms of throughput, the suggested PBO-PEO strategy outperforms other strategies. The evaluation indicates that the suggested PBO-PEO method provides data faster but the existing BSWOA and BFOA provides the data slower. PBO-PEO results in a drop in throughput performance.

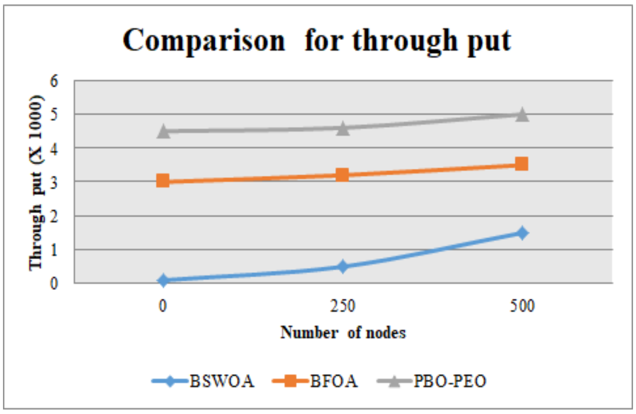

Figure 10: *Comparison for through put*

4.6 Network lifetime

Based on stable and unstable periods the network lifetime is well-defined. Figure 11 shows the comparison of network lifetime with the other networks. The network lifetime is longer for proposed PBO-PEO when compared to the existing BSWOA and BFOA method.

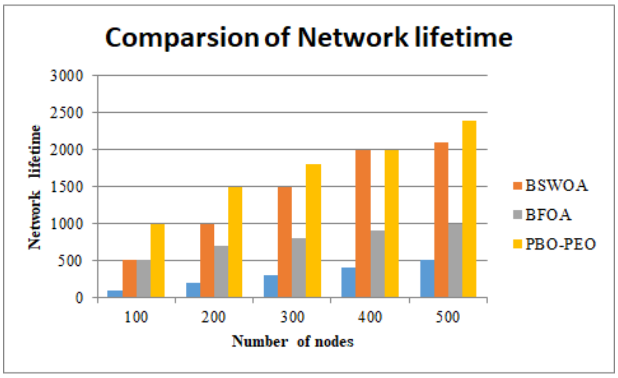

Figure 11: *Comparison for network lifetime*

4.7 Delay

The delay mechanism is going on decreasing for the proposed PBO-PEO method but for existing BSWOA, BFOA techniques the delay is going on increasing is illustrated in figure 12.

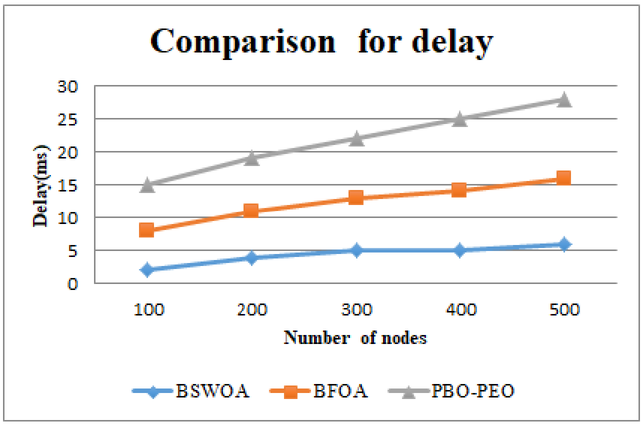

Figure 12: *Delay*

5. Conclusion

The paper presents a robust approach to that leverages fuzzy cluster, Pity Beetle Optimization, and Philippine Eagle Optimization for efficient and secure routing in MANETs. By incorporating a secure routing based on fuzzy-based clustering ensures well-structured, energy-aware group formation, it ensures reliable node identification for routing. The integration of the PBO and PEO-based routing mechanisms significantly enhance path reliability and security. PBO-PEO further enhances routing efficiency, providing optimal path selection whereas maintaining network security. This dual-layered framework effectively addresses challenges such as path management and routing optimization, delivering a secured and high-performance routing mechanism. The proposed PBO-PEO performance is contrasted with those of other optimization techniques, like BSWOA and BFOA. The results showed that the suggested PBO-PEO have a longer network lifetime of 2400, higher throughput of 0.05ms, better energy consumption of 990, and less delay 12ms.

References

1. Sandeep Jagonda Patil; Lalita Sunil Admuthe; Ashwini Sandeep Patil; Saurabh R. Prasad, Year: 2024, "Secure MANET routing with blockchain-enhanced latent encoder coupled GANs and BEPO optimization", Smart Science, Vol: 12, No: 4, pp: 608 – 621.

2. Janaki Sivakumar; Smitha Nayak; Amala Nirmal Doss, Year: 2020, "IoT: Effective Authentication System (EAS) using Hash based Encryption on RFID Attacks", International Journal of Engineering and Management Research, Vol: 10.

3. NS Saba Farheen; Anuj Jain, Year: 2022, "Improved routing in MANET with optimized multi path routing fine tuned with hybrid modeling", Journal of King Saud University-Computer and Information Sciences, Vol: 34, No: 6, pp: 2443 – 2450.

4. GR Rama Devi; M. Swamy Das; MV Ramana Murthy, Year: 2023, "Secure cross-layer routing protocol with authentication key management scheme for manets", Measurement: Sensors, Vol: 29, pp: 100869.

5. N. Saravanan; Rajesh Arunachalam; A. Sahaya Anselin Nisha; A. Karthikayen, Year: 2025, "An innovative energy efficient routing protocol in MANET with hybridized osprey-fire hawk optimization algorithm to attain optimal routing constraints", Wireless Networks, Vol: 31, No: 3, pp: 2005 – 2026.

6. S. Muruganandam; J. Arokia Renjit, Year: 2021, "Real-time reliable clustering and secure transmission scheme for QoS development in MANET", Peer-to-Peer Networking and Applications, Vol: 14, No: 6, pp: 3502 – 3517.

7. Kalaiselvi Gopalasamy; Kavitha Govindarajan Muthaiya, Year: 2025, "Optimizing packet routing and security in MANETs with the H-MAntnetSVM algorithm for energy efficiency and blackhole detection", Sustainable Computing: Informatics and Systems, Vol: 46, pp: 101123.

8. Dilip Kumar Sharma; Ningthoujam Chidananda Singh; Daneshwari A. Noola; Amala Nirmal Doss; Janaki Sivakumar, Year: 2022, "A review on various

cryptographic techniques & algorithms", Materials Today: Proceedings, Vol: 51, pp: 104 – 109.

9. Taj-Aldeen Naser Abdali; Rosilah Hassan; Ravie Chandren Muniyandi; Azana Hafizah Mohd Aman; Quang Ngoc Nguyen; Ahmed Salih Al-Khaleefa, Year: 2020, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET", Information, Vol: 11, No: 11, pp: 529.

10. Uppalapati Srilakshmi; Neenavath Veeraiah; Youseef Alotaibi; Saleh Ahmed Alghamdi; Osamah Ibrahim Khalaf; Bhimineni Venkata Subbayamma, Year: 2021, "An improved hybrid secure multipath routing protocol for MANET", IEEE Access, Vol: 9, pp: 163043 – 163053.

11. Arun Sekar Rajasekaran; S. Shanmuga Priya; Janaki Sivakumar; Akshay Varkale, Year: 2023, "Cybersecurity Measures Using Machine Learning for Business Applications", In 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), pp. 01 – 08, IEEE.

12. Srinivas Aluvala; K. Rajasekhar, Year: 2023, "Secure routing in MANETS using adaptive cuckoo search and entropy based signature authentication", Wireless Personal Communications, Vol: 128, No: 3, pp: 1519 – 1541.

13. D. Sunitha; P. H. Latha, Year: 2025, "A secure routing and black hole attack detection system using coot Chimp Optimization Algorithm-based Deep Q Network in MANET", Computers & Security, Vol: 148, pp: 104166.

14. Varsha Ashok Khandekar; Praveen Gupta, Year: 2025, "Machine learning-based hybrid SSO-MA with optimized secure link state routing protocol in Manet", China Communications, Vol: 22, No: 3, pp: 164 – 180.

15. P. Ravi Kiran Varma; Bura Vijay Kumar; K. L. Hemalatha; Muhammed Basim Jabar; B. M. Manjula, Year: 2023, "Secure Clustering and Routing Based on Modified Whale Optimization Algorithm in MANET", In International Conference on 6G Communications Networking and Signal Processing, pp: 37 – 47. Singapore: Springer Nature Singapore.

16. Neenavath Veeraiah; Osamah Ibrahim Khalaf; C. V. P. R. Prasad; Youseef Alotaibi, Abdulmajeed Alsufyani; Saleh Ahmed Alghamdi; Nawal Alsufyani, Year: 2021, "Trust aware secure energy efficient hybrid protocol for manet", IEEE Access, Vol: 9, pp: 120996 – 121005.

17. Saif Al Rumhi; Janaki Sivakumar, Year: 2023, "Sales Analysis-Review and Recommendations on Business Intelligence", In 2023 24th International Arab Conference on Information Technology (ACIT), pp. 1 – 10. IEEE.

18. Uppalapati Srilakshmi; Saleh Ahmed Alghamdi; Veera Ankalu Vuyyuru; Neenavath Veeraiah; Youseef Alotaibi, Year: 2022, "A secure optimization routing algorithm for mobile ad hoc networks", IEEE Access, Vol: 10, pp: 14260 – 14269.

19. Srivel Ravi; Saravanan Matheswaran; Uma Perumal; Shanthi Sivakumar; Srinivas Kumar Palvadi, Year: 2023, "Adaptive trust-based secure and optimal route selection algorithm for MANET using hybrid fuzzy optimization", Peer-to-Peer Networking and Applications, Vol: 16, No: 1, pp: 22 – 34.

20. G. Arulselvan; A. Rajaram, Year: 2025, "Routing attacks detection in MANET using trust management enabled hybrid machine learning", Wireless Networks, Vol: 31, No: 2, pp: 14.