IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, May 2026
Impact Factor: 8.2

An Enhanced Bacteria Foraging Optimization-Based Trust Model for MANETs

[1]Satish Dagadu Tambe and [2]Dr. Harsh Lohiya
Research Scholar, Department of CSE, SSSTUMS, Sehore, M.P. (India)[1]
Associate Professor, Department of Computer Science & Engineering[2]
Sri Satya Sai University of Technology & Medical Sciences, Sehore

Abstract: *In recent years, the demand for network services has grown significantly, making it increasingly challenging to provide adequate infrastructure, security mechanisms, and reliable access. Mobile Ad Hoc Networks (MANETs) offer a flexible solution by enabling direct communication between two or more nodes without relying on fixed infrastructure. In this study, we propose an optimization method to enhance connectivity between nodes by incorporating a trust-based communication approach to determine optimal routing paths and hop counts for efficient data transmission from source to destination. The proposed Enhanced Bacteria Foraging Optimization Algorithm (EBFOA) focuses on evaluating the reliability and security of nodes within the network. Simulation results under standard conditions demonstrate that the proposed method improves performance and efficiency compared to existing approaches.*

Keywords: Bacteria foraging Optimization Algorithm, Cognitive Radio, Internet of Things, MANET, VANET

I. INTRODUCTION

A mobile adhoc network (MANET) enables wireless communication among devices without relying on fixed infrastructure, forming a network of wireless nodes or sensors. In such networks, a group of nodes dynamically communicates across changing locations, with each node having its own energy constraints and operational lifetime. To ensure efficient communication and organized packet delivery, various routing algorithms and protocols are employed. These protocols are generally categorized into reactive, proactive, and hybrid types. Due to the dynamic and randomly changing topology of MANETs, managing transmission power for data packets becomes a critical challenge. Additionally, nodes within the network must contend with potential security threats and attacks.

Attackers in a MANET environment may originate either from within the network or from external sources. Ensuring reliable communication involves optimizing factors such as packet delivery cost, end-to-end delay, node density, and energy efficiency, all of which contribute to overall quality of service. To address these challenges, advanced techniques including data mining, artificial intelligence, machine learning, genetic algorithms, deep learning models, and bio-inspired optimization methods are widely applied.

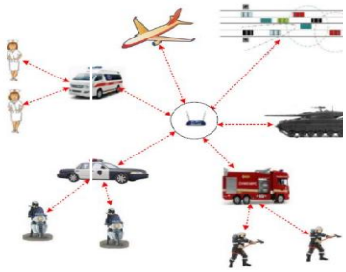

Fig. 1: Mobile ad-hoc network [7].

DOI: 10.48175/568

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 11, May 2026 Impact Factor: 8.2

Over the past two decades, technological advancements have significantly transformed various sectors. Among these, artificial intelligence and optimization methods have emerged as key tools for improving system performance. In this context, several bio-inspired optimization techniques have been explored for mobile ad hoc networks to enhance their efficiency and overall functionality. This work focuses on analyzing such bio-inspired algorithms and demonstrates their effectiveness in improving quality of service parameters compared to existing approaches.

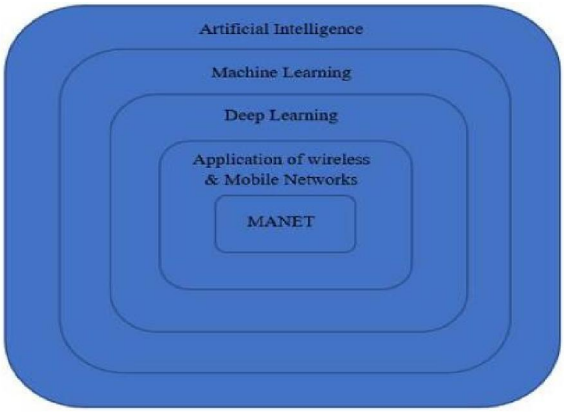

Fig. 2: The above picture represents a relationship between artificial intelligence and mobile ad- hoc network [3].

II. PROPOSED WORK

Biologically inspired methods are widely applied to address resource allocation challenges and enhance quality of service in mobile ad hoc networks. As discussed earlier, such networks face several critical issues, including efficient bandwidth usage, reliability, scalability, and node mobility. In this section, we present our approach, which is based on a bio-inspired optimization algorithm designed to achieve better performance compared to existing methods. The proposed framework incorporates a trust-based mechanism to evaluate nodes alongside the optimization process.

These techniques offer advantageous properties such as adaptability and scalability, making them suitable for dynamic network environments. The primary objective of this work is to determine an optimal solution while ensuring secure communication by identifying trustworthy nodes and minimizing the risk of attacks through a trust-based routing strategy. The model is built upon an enhanced bacteria foraging optimization algorithm and organizes its operations into structured stages for data transmission and route establishment among nodes. Furthermore, it employs the ad hoc on-demand distance vector routing protocol to handle packet transmission, while maintaining routing tables that are continuously updated based on the trust levels of individual nodes.

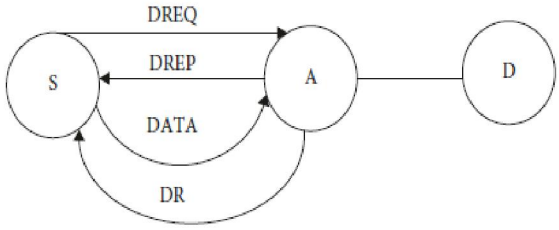

Fig. 3: Data transmission using improved bacteria for aging optimization algorithm based on ad- hoc protocol.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, May 2026
Impact Factor: 8.2

In the above figure node S is a source node, node D is a destination node, and node A is an intermediate node between a source node and the destination node. Here the data sending from the source node is always done only after checking the trust value of node A and sent the message data request to intermediate node A if intermediate node A is reply with a data reply message to node S after checking the congestion in a network, energy availability as required for the successful forwarding of a packet, and also check the node status which is a malicious node or not, if the node is marked with malicious node then source node discards the data sending process via an intermediate node. After receiving successful packets from the source node, node A forwards the packet to destination node D.

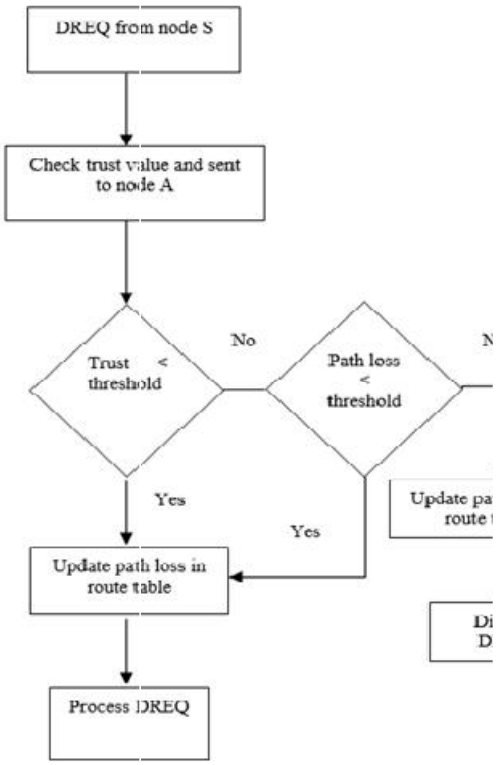

Fig. 4: The above figure represents the trust-based mechanism for forwarding a packet from the source node to the destination node.

In the above figure, we represent our proposed work model which is based on the trust-based value, the node is always checking a trust value before forwarding the packets, and its compared with a threshold value, if a node value is less than the threshold value then we use respective node is a trusted node otherwise not if a node is trusted then intermediate node reply the date request otherwise the request is discarded.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, May 2026
Impact Factor: 8.2

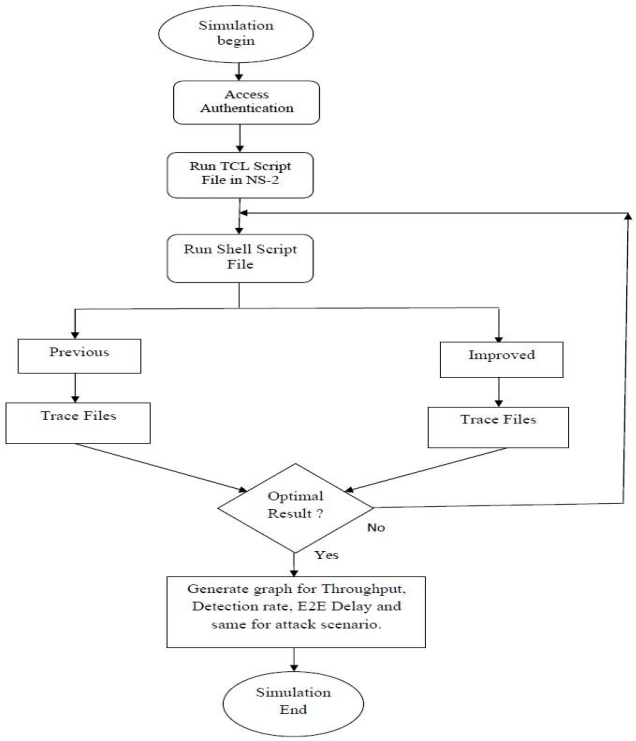

Fig. 5: The above figure presents the proposed workflow graph.

There are some steps we have to follow to implement this system are following:-

Step 1- begin the process of virtualization and open the VMware machine and turn on the power of the virtual machine.

Step 2- After the successful power on for the machine log in with the id and password to enter into the machine.

Step 3- Run the tool command script file for the network simulator.

Step 4- Open the shell scripting window and run the file using the shell command.

Step 5- Apply the techniques with the network simulator s like the previous approach and proposed approach.

Step 6- Find the best route according to the applied techniques with the network simulator and find the best route or path.

Step 7- Getting the optimal routing results.

Step 8- After getting optimal results if we are not satisfied with the results then go to step 5, until we found the best results.

Step 9- Exit the experimental simulation process and end the VMware machine with a power-off signal.

III. RESULT ANALYSIS

In this section, we discuss the proposed experimental results compare with the existing techniques; also discuss the simulation experimental environment and the snapshot for the proposed and existing methods results. The proposed methods give better results than the currently existing techniques, the performance evaluation parameters are such as the delay between the packets are transmitting between a source node and destination node, throughput for a delivered number of packets, and packet delivery ratio for a packet between the source and destination, here we discuss comparative performance result summary using existing and proposed methods with tabular form and graphical representation also.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, May 2026
Impact Factor: 8.2

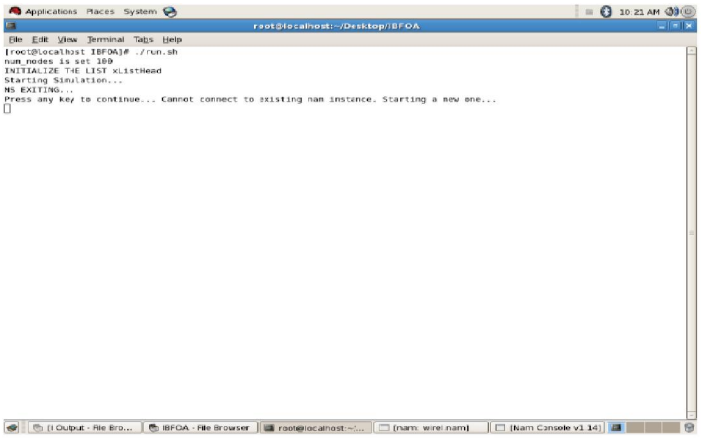

Fig. 6: This window shows the running shell files output and their description used in a network simulator.

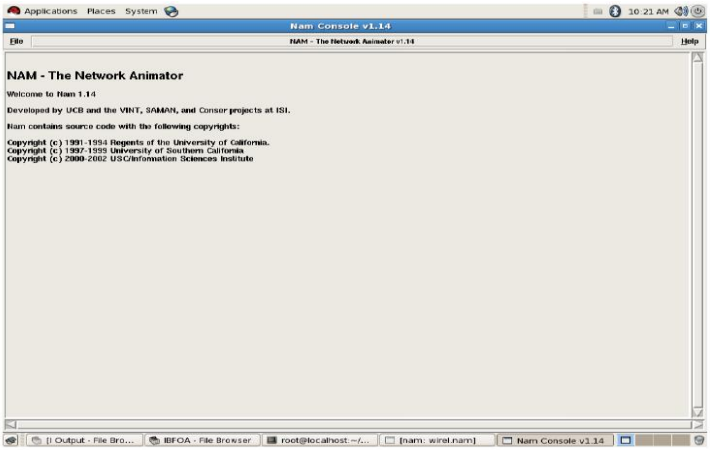

Fig. 7: The above window shows the network animator files in a network simulator.

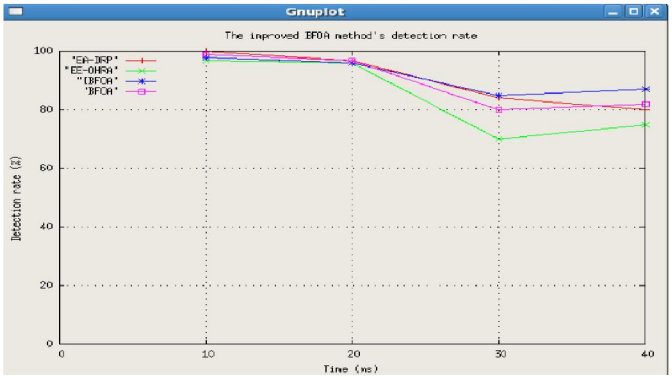

Fig. 8: The above window shows the output of a performance parameter is the detection rate for the existing and proposed method in a network simulator.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 11, May 2026
Impact Factor: 8.2

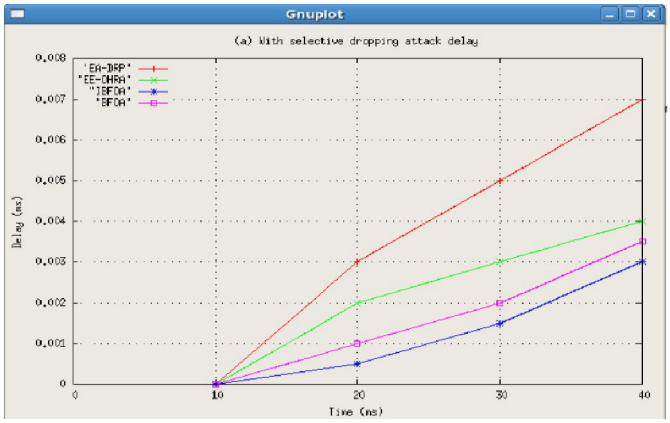

Fig. 9: The above window shows the output of a performance parameter a delayed with a selective dropping attack for the existing and proposed method in a network simulator.

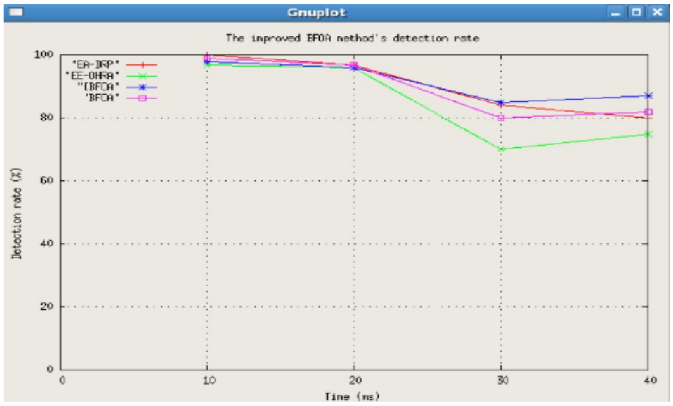

Fig. 10**:** The above window shows the output of a performance parameter is detection rate for the existing and proposed method in a network.

IV. CONCLUSION

This paper presents experimental results demonstrating improved quality of service compared to existing approaches. The proposed algorithm identifies reliable nodes based on their trust values, enabling secure communication across the network. Simulation studies are conducted under both normal and attack conditions, and the results indicate that the proposed method outperforms current techniques in terms of overall performance.

REFERENCES

[1] Uppalapati Srilakshmi, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, Youseef Alotaibi, “A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks”, IEEE Access, 2022, pp. 14260-14269.

[2] Uppalapati Srilakshmi, Neenavath Veeraiah, Youseef Alotaibi, Saleh Ahmed Alghamdi, Osamah Ibrahim Khalaf, Bhimineni Venkata Subbayamma, “An Improved Hybrid Secure Multipath Routing Protocol for MANET”, IEEE Access, 2021, pp. 163043-163053.

[3] Raghu Ramamoorthy, Menakadevi Thangavelu, “An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks”, Journal of Ambient Intelligence and Humanized Computing, 2022, pp. 1-34.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 11, May 2026 Impact Factor: 8.2

[4] Shahenda Sarhan, Shadia Sarhan, "Elephant Herding Optimization Ad Hoc On-Demand Multipath Distance Vector Routing Protocol for MANET", IEEE Access, 2021, pp. 29489-29499.

[5] K. Sakthidasan Sankaran, N. Vasudevan, K. R. Devabalaji, Thanikanti Sudhakar Babu, Hassan Haes Alhelou, T. Yuvaraj, "A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks", IEEE Access, 2021, pp. 21735-21745.

[6] Baidaa Hamza Khudayer, Mohammed Anbar, Sabri M. Hanshi,Tat-Chee Wan, "Efficient Route Discovery and Link Failure Detection Mechanisms for Source Routing Protocol in Mobile Ad-Hoc Networks", IEEE Access, 2020, pp. 24019-24033.

[7] Ahuja, Y, Rathore, D. , Mishra S K , "Efficient Routing Scheme for Vehicular Ad-hoc Network using Dedicated Short Range Communication Protocol", International Journal of Emerging Technology and Advanced Engineering, Vol-9, Issue-10, pp. 110-113.

[8] Valmik Tilwari, R. Maheswar, P. Jayarajan, T. V. P. Sundararajan, MHD Nour Hindia, Kaharudin Dimyati, Henry Ojukwu,, Iraj Sadegh Amiri, "MCLMR: A Multicriteria Based Multipath Routing in the Mobile Ad Hoc Networks", Wireless Personal Communications, 2020, pp. 1-24.

[9] Burhan Ul Islam Khan, Farhat Anwar, Rashidah Funke Olanrewaju, Bisma Rasool Pampori, Roohie Naaz Mir, "A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks", IEEE Access, 2020, pp. 124097-124109.

[10] Xiaoliang Wang, Peng Zhang, Yuyue Du, Mei Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network", IEEE Access, 2020, pp. 47675- 47694.

[11] Masood Ahmad, Abdul Hameed, Ataul Aziz Ikram, Ishtiaq Wahid, "State-of-the-Art Clustering Schemes in Mobile Ad Hoc Networks: Objectives, Challenges, and Future Directions", IEEE Access, 2019, pp. 17067-17084.

[12] Anchal Thakur, Deepak Rathore, "Analyze the Performance of Bio-Medical Image Compression Technique using Particle Swarm Optimization", International Conference on Advanced Computation and Telecommunication, 2018, IEEE, pp. 1-4.

[13] Hyun-Ho Choi, Jung-Ryun Lee, "Local Flooding-Based on-Demand Routing Protocol for Mobile Ad Hoc Networks", IEEE Access, 2019, pp. 85937-85951.

[14] R Dubey, D Rathore, D Kushwaha, JP Maurya, "An empirical study of intrusion detection system using feature reduction based on evolutionary algorithms and swarm intelligence methods", International Journal of Applied Engineering Research 12 (19), 2017. pp. 8884-8889.

[15] Ibrahim Kacem, Belkacem Sait, Saad Mekhilef, Nassereddine Sabeur, "A New Routing Approach for Mobile Ad Hoc Systems Based on Fuzzy Petri Nets and Ant System", IEEE Access, 2018, pp. 65705-65720.

[16] T. Poongodi, Mohammed S. Khan, Rizwan Patan, "Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks", IEEE Access, 2019, pp. 18409-18420.

[17] Dinesh Chander, Rajneesh Kumar, "QoS Enabled Cross-Layer Multicast Routing over Mobile Ad Hoc Networks", International Conference on Smart Computing & Communication, 2018, pp. 215-227.

[18] Ishtiaq Wahid, Ataul Aziz Ikram, Masood Ahmad, Sajjad Ali, Arshad Ali, "State of the Art Routing Protocols in VANETs: A Review", Procedia Computer Science, 2018, pp. 689-694