ISSN: 2581-3404 (Online) IF: 5.68 (SJIF)
IJIRTM, Volume-9, Issue-3, June-2025

A Secure Communication in MANET Using Trust Based Mechanism

Sourabh Singh[1], Dr. Puneet Nema[2]
[1]M. Tech. Research Scholar, Department of CSE, LNCT, Bhopal, M.P. (India).
[2]Assistant Professor, Department of CSE, LNCT, Bhopal, M.P. (India).

Abstract. *The mobile ad-hoc network (MANET) is dynamically formed by wireless mobile nodes that arbitrarily move without the administration of a base station or any central point. MANET is considered as a multi-hop network; within a multi-hop network, the source node can communicate with its destination through intermediate nodes because the destination is out of the communication range of the source node The proposed algorithm which is based on the find right node according to their trust value and make a secure communication between the nods in a network, here in simulation scenario present the experimental result for the normal mode and as well as attack mode, and find the better performance.*

Keywords: Optimization Algorithm, Internet of Things, Mobile ad hoc network, Vehicular Ad hoc Networks.

Introduction

The mobile ad-hoc network (MANET) is dynamically formed by wireless mobile nodes that arbitrarily move without the administration of a base station or any central point. MANET is considered as a multi-hop network; within a multi-hop network, the source node can communicate with its destination through intermediate nodes because the destination is out of the communication range of the source node [1]. Wireless networks have experienced significant growth in popularity over the past decades, with two primary variations: infrastructure networks and infrastructure-less networks. Infrastructure networks, such as cellular networks and wireless local area networks (IEEE 802.11), rely on centralized controllers to establish and maintain communications between terminals. In contrast, infrastructure-less networks, also known as wireless ad hoc networks, operate in a decentralized manner. Terminals within an ad hoc network can autonomously establish connections and communicate with each other in a multi-hop fashion without relying on fixed infrastructure.

This inherent infrastructure-less property enables rapid deployment and robust operation, making ad hoc networks suitable for applications such as emergency services, disaster recovery, wireless sensor

networks, and home networking. Effective communication plays a vital role in facilitating information exchange among individuals in various contexts and locations. Mobile Ad Hoc Networks (MANETs) are a collection of mobile nodes that form a network independently, without centralized administration. However, as these mobile devices operate on batteries, extending their battery life has become a critical objective.

Literature Review

In this research work, the Bacteria for Aging Optimization Algorithm (BFOA), which finds the ideal hops in advancing the routing, is utilized to offer a trust-based protected and energy-efficient navigation in MANETs using a trust-based protected and energy efficient navigation algorithm [2]. The fuzzy clustering algorithm is activated first, and the Cluster Heads (CHs) are selected depending on the value of indirect, direct, and recent trust that each CH has. In addition, value nodes were discovered based on trust levels. Moreover, the CHs are engaged in multi hop routing, and the selection of the ideal route is based on the projected protocol, which selects the best routes based on latency, throughput, and connection within the course's boundaries. The routing protocol Genetic Algorithm with Hill climbing (GAHC) described in this article shows a hybrid GA-Hill Climbing algorithm that picks the optimal route in multipath. Prior to this in the beginning, the Improved fuzzy C-means algorithm method was built on density peak, and cluster heads (CHs) were chosen in a predicted manner, based on recent, indirect, and direct trust [3]. The computation is based worth nodes are at the trust threshold found in addition. Even CHs take part in the alternate paths, the blend of all the many paths from these Cluster Heads that chooses the optimal route, which is based on the predicted hybrid protocol, as well as the optimum route's aggregate features such as throughput, latency, and connection. In this research article, they propose an Enhanced Hybrid Ant Colony Optimization Routing Protocol (EHACORP) to improve the efficiency of the routing process using the shortest path. The shortest path in the proposed protocol has low communication costs and the least number of hops between source and destination vehicles [4]. The EHACORP has two phases. In phase 1, the EHACORP relies on a distance calculation method to compute the distance between vehicles. In phase 2, the source based ant colony optimization is used to guide the ants to build a shorter path with the least number of hops to transmit data. The shortest path improves the efficiency of protocol in all aspects. In this research work, they propose energy efficient routing protocol based on the well-known Ad Hoc On-Demand Multipath Distance Vector (AOMDV) routing protocol and a bio-inspired algorithm called Elephant Herding Optimization (EHO). In the proposed EHO-AOMDV the overall consumed energy of nodes is optimized by classifying nodes into two classes, while paths are discovered from the class of the fittest nodes with sufficient energy for transmission to reduce the probability of path failure and the increasing number of dead nodes through higher data loads [5]. The EHO updating operator updates classes based on separating operator that evaluates nodes based on residual energy after each transmission round. Experiments were conducted using Ns-3 with five evaluation metrics routing overhead, Mobile ad-hoc network is an assortment of

distinct attribute-based mobile devices that are autonomous and are cooperative in establishing communication. These nodes exploit wireless links for communication that causes injection of the adversaries in the network [6]. Therefore, detection and mitigation of adversaries and anomalies in the network are mandatory to retain its performance. To strengthen this concept, in this article, a novel secure neighbor selection technique using recurrent reward-based learning is introduced. This proposed technique inherits the benefits of conventional routing and intelligent machine learning paradigm for classifying the states of the nodes based on their communication behavior. This research work, aims to enhance on-demand source routing protocols by proposing two mechanisms, a zone-based route discovery mechanism (ZRDM) and a link failure prediction mechanism (LFPM). ZRDM aims to control the flooding of route requests, and LFPM aims to avoid route breakages caused by node mobility [7]. The performance of the proposed mechanisms was evaluated using network simulator 3 in terms of normalized routing load, average end-to-end delay, and packet delivery ratio. The experimental results showed that the proposed mechanisms outperform well-known mechanisms such as the dynamic source routing (DSR) protocol, reliable DSR, and zone-based DSR and segment-based DSR. This research work proposes a routing strategy called Mobility, Contention window, and Link quality sensitive multipath Routing (MCLMR) in MANETs, which considers the nodes mobility, contention window size, and link quality estimated value of the intermediate nodes in the optimal route selection [8].

Proposed Work

Bio-inspired algorithms evolve to achieve a given purpose and obtain an optimal result by following a set of simple and heuristic rules for operation without the aid of a central coordinator. The proposed work with the trust based approach using the optimization techniques. The main objective of this suggested solution is to ensure security in the routing network. The suggested solution is a method of trust-based routing. This system is classified as Data Retrieval (DR) Table Stage and Route Formation Stage. The proposed system, as shown in below figure, Ad-hoc On-Demand Distance Vector (AODV) protocol, is used to pass data packets to a mobile network and retains a different route table.

For reliable data delivery, this proposed protocol scheme uses the concept of acknowledgment packets. Whenever the source intends to send packets to its neighbor, it sends DREQ packet to its neighbor requesting its neighbor node’s status. If the neighbor node is active, it immediately responds with the DREP packet. After receiving the DREP packet, the source node sends its data. After completion of data transmission, the source node expects acknowledgment from the neighbor node. After receiving the data, the neighbor node sends DR packet to the source node. This data transmission process continues till all the packets sent by the source node reach the destination successfully. Finally, one acknowledgment packet is sent to the source from the destination node after receiving all the packets. Once the source gets an acknowledgment from the destination node, it considered the route and the intermediate nodes across the route are trusted, and at the same time, trust values are updated. In this way, the proposed scheme

ensures reliable packet transmission by minimizing the packet loss; hence, the throughput of the network can be intensified.

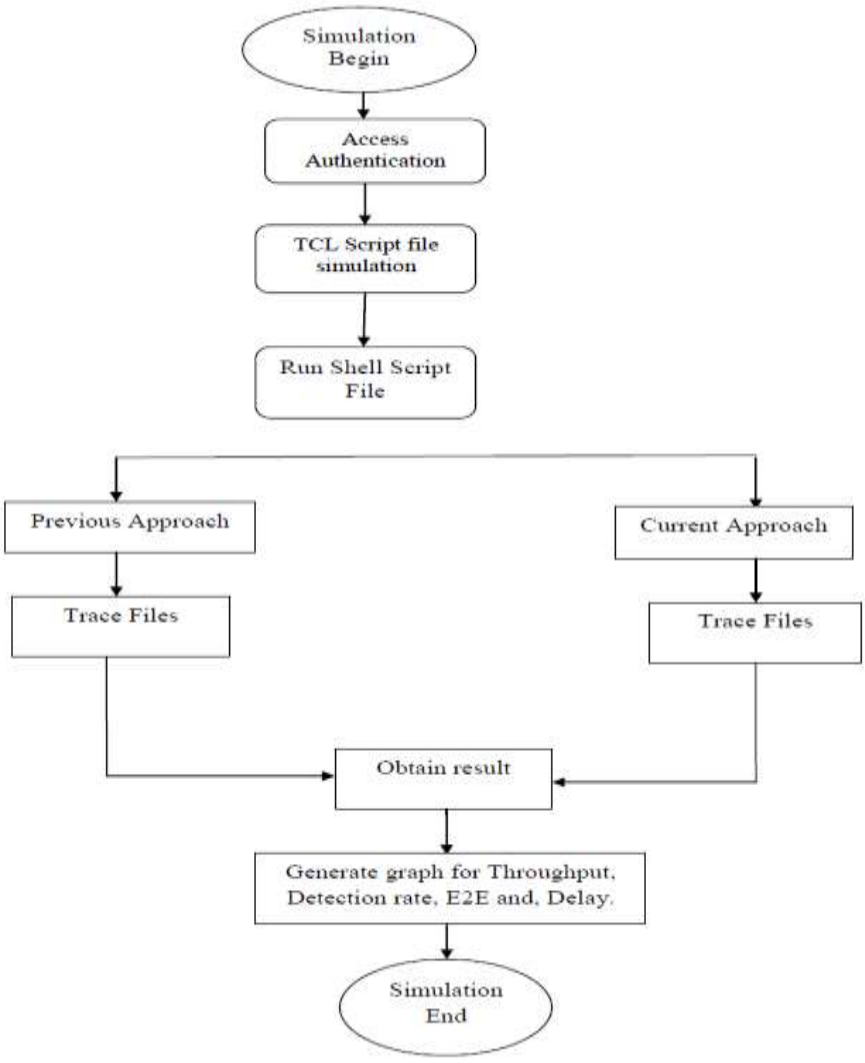

Figure 1: The above figure present the proposed work flow graph.

Experimental Work

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

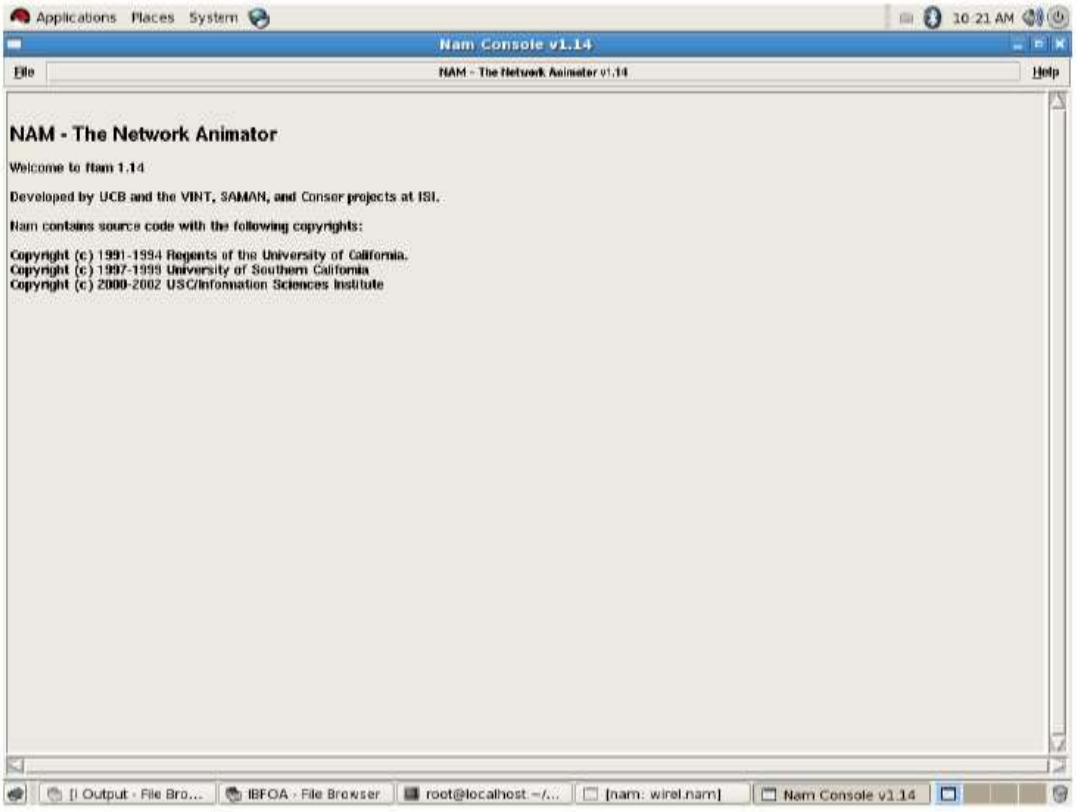

Figure 2: This picture shows the network animator files in a network simulator.

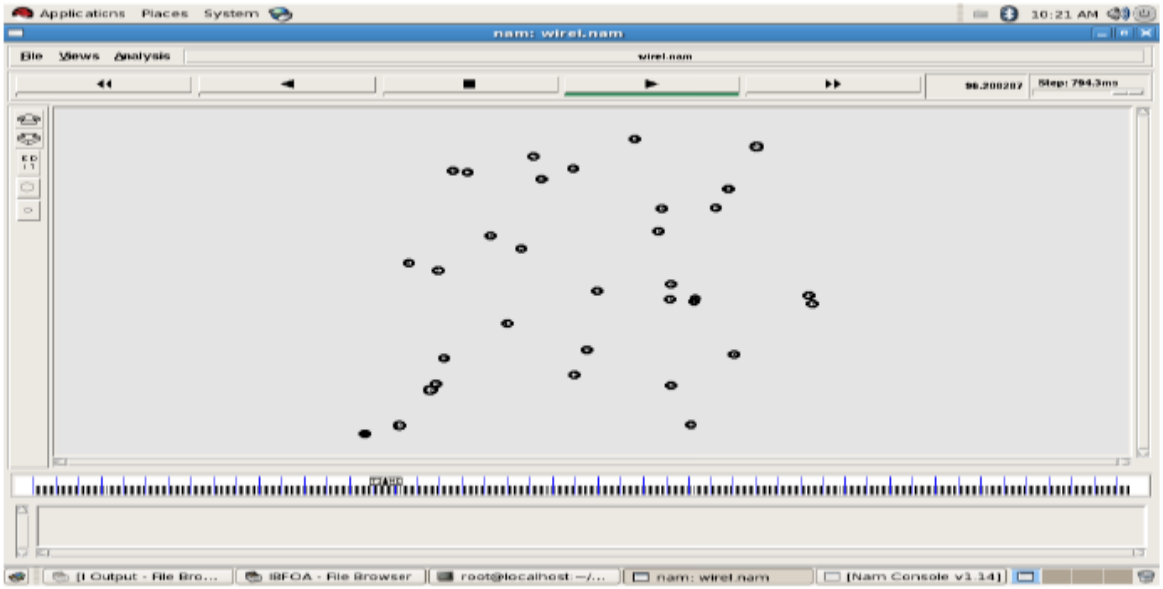

Figure 3: This picture shows the different nodes in a network animator files.

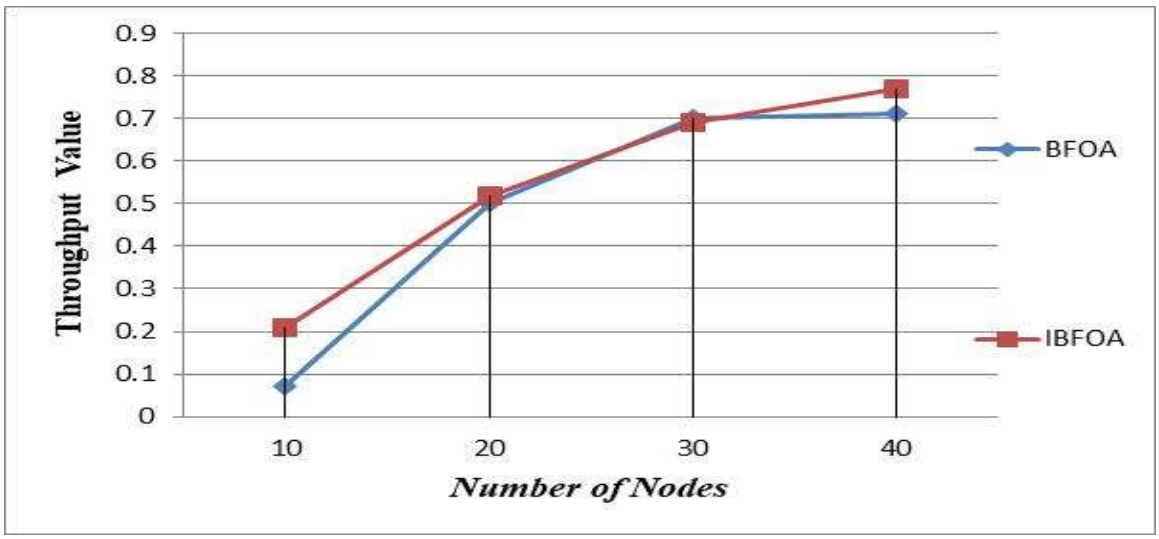

Figure 4: This picture represents throughput value between source node to destination node for previous approach and proposed approach.

Conclusion

The use of wireless connections and the flexibility of different devices in such networks have a number of significant implications, and many well-known intrusion-detection processes and implementations do not instantaneously become invisible from infrastructure-based internet protocol (IP) address networks. In this work present an improved Bacteria for Aging Optimization Algorithm (BFOA), which finds the ideal hops in advancing the routing, is utilized to offer a trust-based protected and energy-efficient navigation in MANETs using a trust-based protected and energy efficient navigation algorithm. The proposed algorithm which is based on the find right node according to their trust value and make a secure communication between the nods in a network, here in simulation scenario present the experimental result for the normal mode and as well as attack mode, and find the better performance than the existing techniques.

References

[1] David Airehrour, "A Cluster-Driven Energy Routing Protocol for Optimal Network Lifetime in Ad Hoc Networks", Journal of Telecommunications and the Digital Economy, 2019, pp. 16-30.

[2] 1Arash.Ghafouri, Ahmad Ghasemi, Mohammad Rez, Hasani Ahangar, "A Power-based Method for Improving the ODMRP Protocol Performance in Mobile Ad-hoc Networks", I.J. Wireless and Microwave Technologies, 2018, pp. 27-36.

[3] D. Kothandaraman, C. Chellappan, "Energy Efficient Node Rank-Based Routing Algorithm in Mobile Ad-Hoc Networks", International Journal of Computer Networks & Communications, 2019, pp. 45-63.

[4] Mina Ghafouri vaighan & Mohammad Ali Jabraeil Jamali, "A multipath QoS multicast routing protocol based on link stability and route reliability in mobile ad-hoc networks", Journal of Ambient Intelligence and Humanized Computing, 2017, pp. 4-20.

[5] J.D. Abdulai, K. S. Adu-Manu, F. A. Katsriku, F. Engmann, "A modified distance-based energy-aware (mDBEA) routing protocol in wireless sensor networks (WSNs)", Journal of Ambient Intelligence and Humanized Computing, 2022, pp. 1-23.

[6] M.Rajesh, "A Review on Excellence Analysis of Relationship Spur Advance in Wireless Ad Hoc Networks", International Journal of Pure and Applied Mathematics, 2018, pp. 407-412.

[7] Vu Khanh Quy, Vi Hoai Nam, Dao Manh Linh, Nguyen Tien Ban, Nguyen Dinh Han, "Communication Solutions for Vehicle Ad-hoc Network in Smart Cities Environment: A Comprehensive Survey", Wireless Personal Communications, 2022, pp. 2791-2815.

[8] Laji Merin Varkey, Ashish Gupta, "Multipath AODV Implementation in Wireless Ad hoc Network for Improved Performance", International Journal of Innovative Research in Science, Engineering and Technology, 2023, pp. 3830-3836.

[9] Vu Khanh Quy, Nguyen Tien Ban, Nguyen Dinh Han, "A Multi-metric Routing Protocol to Improve the Achievable Performance of Mobile Ad Hoc Networks", Springer, 2018, pp. 445-454.

[10] S. Venkatasubramanian, Dr. A. Suhasini, C.Vennila, "An Energy Efficient Clustering Algorithm in Mobile Adhoc Network Using Ticket Id Based Clustering Manager", International Journal of Computer Science and Network Security, 2022, pp. 341-349.

[11] Folayo Aina, Sufian Yousef, Opeyemi Osanaiye, " Analysing admission control for AODV and DSR routing protocol in mobile ad-hoc network", Bulletin of Electrical Engineering and Informatics, 2021, pp. 2667-2677.

[12] Bata Krishna Tripathy, Swagat Kumar Jena, Padmalochan Bera, Satyabrata Das, "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks", 2020, pp. 1-32.