AN INTEGRATED SECURED ROUTING APPROACH FOR MANETS

Dr. D. CHITRA, DIVYA.K

Dr.D. Chitra, Professor, Department of Electronics and Communication engineering Mahendra Engineering College
Divya K, PG student, Department of Electronics and Communication Engineering, Mahendra Engineering College

---***---

Abstract

This paper aims to integrate different machine learning algorithms to get an optimized and secured routing technique for Mobile Ad-hoc NETworks(MANETs). Routing of packets are highly challenging in MANETs, as they are infrastructure-less networks formed with mobile nodes, connected by flexible wireless links. The main routing challenges in MANETs are the frequent topological changes, limited availability of power resources and vulnerabilities to attacks. This method suggests a technique that is trustworthy that provides fast convergence for topological changes with minimum energy utilization per packet. In this method, a trust-based and energy-efficient fuzzy clustering routing algorithm is used. The Cluster Heads(CHs) are selected depending on the various trust values that provide multi-paths to the destination. Then Bacteria for Aging Optimization Algorithm (BFOA) selects the best path by finding ideal hops to the destination avoiding the misbehaving nodes. The proposed method offers better security, reduced delay and better energy utilization.

Keywords: Cluster heads, Trust model, BFOA, Intruder detection, Misbehaving nodes.

1. Introduction

The MANETs are flexible wireless networks with dynamic topology. The MANETs are formed through the collection of mobile nodes which are connected with wireless links. The topology of MANET changes as the mobile nodes enter and leave the network. When a node along a path leaves the network, the packets along that route must be routed through another alternate path. These frequent topology changes and related routing problems are the major issues in the development of routing protocols for MANETs. The second design issue is related to the power resources availability. The mobile devices depend on one or another form of the exhaustible power source. When the power supply is exhausted at a node, it becomes a dead node and cannot take part in the transmission of the packets. The other problem is the presence of attackers inside and outside the network. In MANETs, there is no centralized monitoring mechanism to detect and prevent intruders.

Here, we propose an integrated approach to solve the routing issues in MANETs. This method uses a fuzzy clustering algorithm that determines the CHs through an effective adaptive trust model. As it selects the nodes with maximum trust values and sets the threshold for trust values, the intruder nodes can be easily and effectively identified. It provides multiple paths between the source and destination. In the second stage, an optimal route is selected employing BFOA that uses ideal hops to determine the route.

2. Related works

In paper [1], M. Jabirulla and A. Kumar discuss how to plan and analyze obstacles, mobility, and power for optimal MANET routing. It uses a routing protocol framework to uncover viable investigations of obstacles, power, and mobility. The paper aims to solve issues caused by mobility, interface quality, and battery imperative of mobile hubs between overlay associations. The proposed method selects routing choices by deciding the optimal course with energy-productive hubs to keep up network dependability and lifetime. The power mindful utilizations obstacle recognition algorithm for the choice of optimal middle-of-the-road hubs dependent on the available energy level, mobility, and connection quality boundaries. In Mobile Ad Hoc Networks (MANETs), the absence of centralized infrastructure, changes in the network topology, device mobility and data transmission over wireless channels make multi-hop routing a very challenging task. The MANETs can be deployed in many critical applications and developing a routing protocol that deals with these challenges through the design of a Quality of Service (QoS)-assured protocol is a major problem. As the movement of mobile nodes in MANETs occurs frequently, a proper approach with robustness and QoS assurance is required. S. Mostafavi *et. al.* [2] proposed QMAR-AODV, which is an optimized version of the AODV protocol called the QoS-assured Mobility-Aware Routing protocol. It outperforms E2E-LREEMR and reduces route instability, end-to-end delay, data retransmissions and packet loss while increasing data reception and network throughput, compared to E2E-LREEMR routing protocol. There is a need for a secure protocol for MWSN with mechanisms that take into account the limited resources of the nodes and the dynamism of its nodes' locations which are included in the research of O. Oladayo and A. Ashraf [3]. Background and Objective Mobile Wireless Sensor Network (MWSN) is a specialized wireless network made up of a large number of mobile sensors, where each sensor is capable of changing its location and relaying data to either the base station or neighbouring nodes. Therefore it is not suitable for WSN that is energy-constraint with mobile sensors. This protocol is capable of selecting the optimal multi-hop route among available routes for the source node and securely hops the data to the destination nodes through intermediary nodes. To make sure about the security level of the protocol, formal and informal security analysis of the routing protocol is done.

The development of Remotely Piloted Aircrafts (RPAS) for civil applications has been rapidly growing over the past years. To achieve this task a two-layered approach is proposed [4]. The Ant Colony Optimization(ACO) which is based on Swarm Intelligence(SI) are well suited for MANETs. An inexpensive and feasible solution for real-world implementation is provided by the Potential Field method. It is shown that the algorithms perform reasonably well in several scenarios. Even though the network assumes that all its mobile nodes are trusted, it is impossible in the real world as few nodes may be malicious. Therefore, it is essential to put forward a mechanism that can provide security by selecting an optimal route for data forwarding as suggested by A. M. Chintalapalli and V. R. Ananthula[5]. A fitness function is developed for the selection of the best routes using the multi-objective parameters. The performance of this algorithm is evaluated using three metrics, such as packet delivery ratio (PDR), throughput, and energy and is compared with that of existing trust-based QoS routing model, LA, and WOA. Energy harvesting is crucial for IoT devices as it eliminates the need for frequent energy source replacement. With advancements in EH techniques, the design procedures of routing protocols have undergone a dramatic change for energy-harvesting wireless sensor network-based IoT applications. T. D. Nguyen *et. al.* [6] proposed a new routing algorithm called EHARA that improves energy efficiency and satisfies QoS requirements of distributed IoT networks. In [7], a noble route selection technique based on the mobility of the nodes in ad-hoc networks are presented. The mobility factor is used to select nodes to establish a path between source and destination nodes. Simulations of dynamic source routing and ad hoc on-demand distance vector routing protocols with and without the proposed technique show that the proposed protocols outperform existing protocols.

The remaining part of this paper is organized as : Section III describes the methodology Section IV the Output and Section V gives the Conclusion.

3. The Methodology

An efficient MANET routing technique provides the transmission of data packets without much delay and without any loss. In the proposed method, the use of BFOA reduces the transmission energy losses and enhances the system's lifetime.

The various steps used in this method are:

1. Application of fuzzy clustering algorithm and selection of CHs based on direct, indirect and recent trust values.
2. Application of BFOA algorithm for the optimum route selection avoiding the intruder nodes.

3.1 CH selection

Using the fuzzy clustering algorithm CHs are selected based on the direct, indirect and recent trust values. The trust management mechanism is very effective to deal with security issues in MANETs. The traditional trust management systems are not effective, as frequent communication may lead to congestion, high energy consumption and large transmission delay between the source and destination. In this method, the use of adaptive factors with space and time constraints improves the accuracy of the trust value evaluation and also speeds up the detection of malicious nodes. Using the CH formation secure multi paths can be obtained and the best secure path avoiding the misbehaving nodes is selected using BFOA.

Trust values indicate the degree of trust depending on the behaviour of the nodes. A trust model is composed of the following 5 components.

Trust Composition – This involves the computation of the trust values.
Trust formation – It determines the trust attributes for the computation of the trust values.
Trust propagation – It represents the ways in which trust information is propagated to other nodes.
Trust aggregation – It aggregates trust information from the various trust values such as direct, indirect and recent trust values.
Trust update – It determines when the trust values are to be updated using trust aggregation.

Direct Trust (DT): It is the difference between the actual time and predicted time for the i^{th} node to authenticate the public key that was generated by the k^{th} destination node.

InDirect Trust (IDT): DT depends on the information exchanged between the neighbouring nodes. If the communication is not effective or the channel or the neighbouring nodes are malicious, then DT values cannot measure the credibility of the nodes.

$$IDT_i^k(t) = \frac{1}{n}\sum_{i=1}^{n} DT_i^k(d) \qquad (1)$$

where n is the number of neighbouring nodes of i^th node.

Recent Trust(RT): Recent trust values are used for local trust synthesis. RT is designed to be

$$RT_i^k(t) = \alpha * DT_i^k(t) + (1-\alpha) * IDT_i^k(t) \qquad (2)$$

where $\alpha = 0.3$

3.2 The BFOA

The bio-inspired BFOA is used to identify the ideal hops for the ideal route selection for MANETs. BFOA can be used to solve several difficult numerical problems quickly and effectively. For searching the nutrients, a bacterium uses a process called Chemo taxis to follow a path. To stimulate the chemo-toxic movement, the bacteria communicate with each other through signals. The underlying optimization method can be used to solve numerous optimization problems. Bacteria can tumble or swim to travel with the help of Flagella. When placed in a semi-solid matrix with a single chemo-effector, a group of E. coli cells arrange themselves in a traveling ring by moving up the nutrient gradient. The cells aggregate into groups when they are stimulated by a high level of succinate and move as concentric swarm patterns. This is called swarming. This process continues for the entire life span. The cell-to-cell signalling can be represented by an objective function. In the reproduction stage, the less healthy bacteria will die and healthier bacteria go to the next generation by breaking into two, which are placed in the same location. This mechanism keeps the swarm size stable. Elimination and Dispersal is the stage where a bacterium population undergoes a gradual or sudden change. Due to various reasons, there may be a gradual or sudden changes in the bacterium population lives. In some cases, all the bacteria in a region are killed or a group is moved into a new location.

The BFOA Algorithm

Step 1: All variables are initialized, and counters are set for the elimination-dispersal loop(l), reproduction loop(k), chemotactic loop(j) and swim counter(w) is set to zero Step 2: Bacterium index (i) is set to zero Step 3: Elimination-dispersal loop is started by setting l = l + 1 Step 4: Start the reproduction loop by setting k = k + l Step 5: Start the chemotaxis loop by setting j = j + 1

Step 1: Initialize all variables and set counters for elimination-dispersal loop(l), reproduction loop(k), chemotactic loop(j) and swim counter(w)

Step 2: Start the elimination-dispersal loop

Step 3: Start the reproduction loop

Step 4: Start the chemotaxis loop, compute the fitness function and go to next bacterium to process next.

Step 5: Continue chemotaxis if the lifespan of the bacteria is not over.

Step 6: Start the reproduction process

Step 7: Start the next-generation process.

Step 8: Eliminate and disperse each bacterium to keep the number of bacteria in the group constant.

Step 9: End if the dispersal loop is completed; otherwise go to step 2.

4. Results and Discussions

This section presents the performance analysis of the suggested method based on different metrics.

Time delay

It represents the end-to-end delay time elapsed from the generation of the packet at the source node to the successful delivery of that packet to the destination. The table 1 shows a comparison of the delays experienced by different methods and we see can see that the proposed method experiences less delay. With an adaptive trust value model, the delay of the packets at the malicious nodes can be avoided.

Table 1 Delay time of existing and proposed methods

Number of nodes	EA-DRP (Sec)	EE-OHRA (Sec)	Proposed method (Sec)
10	80	83	67
20	90	92	85
30	77	79	74
40	89	97	83
50	73	78	69
60	93	98	88

Packet Delivery Ratio (PDR)

PDR represents the ratio of the packets that are successfully delivered to the destination node out of the number of packets that are sent by the source. Table 2 shows a comparative analysis of the PDR.

Table 2 Packet delivery ratio of existing and proposed method

Number of nodes	EA-DRP (%)	EE-OHRA (%)	Proposed method(%)
10	79.5	70.8	83.6
20	77.87	75.7	86.9
30	80.5	78.63	84.5
40	78.08	76.73	87.43
50	81.83	80.72	85.75
60	80.5	81.98	89.85

As the proposed system uses an effective trust management model, misbehaving nodes can be accurately determined. The use BFOA for the best path selection effectively avoids the paths through malicious nodes. This mechanism ensures no packet loss in the transmission which yields a high packet delivery ratio.

Routing Overhead (RO)

The optimal route discovery and successful transmission of the packets demand for more control packets. The comprehensive trust values of the trusted neighbouring nodes calculated by the sink nodes reduce the network overheads and thus reduces congestion. The routing overhead of existing and proposed methods have been summarized in table 3.

Table 3 Routing Overhead of existing and proposed methods

Number of nodes	EA-DRP (%)	EE-OHRA (%)	Proposed method (%)
10	33.5	30	27.4
20	28.7	29.3	25.9
30	31.9	30.4	27.98
40	35.75	33.67	29.54
50	25.8	24.9	20.6
60	37.06	34.7	25

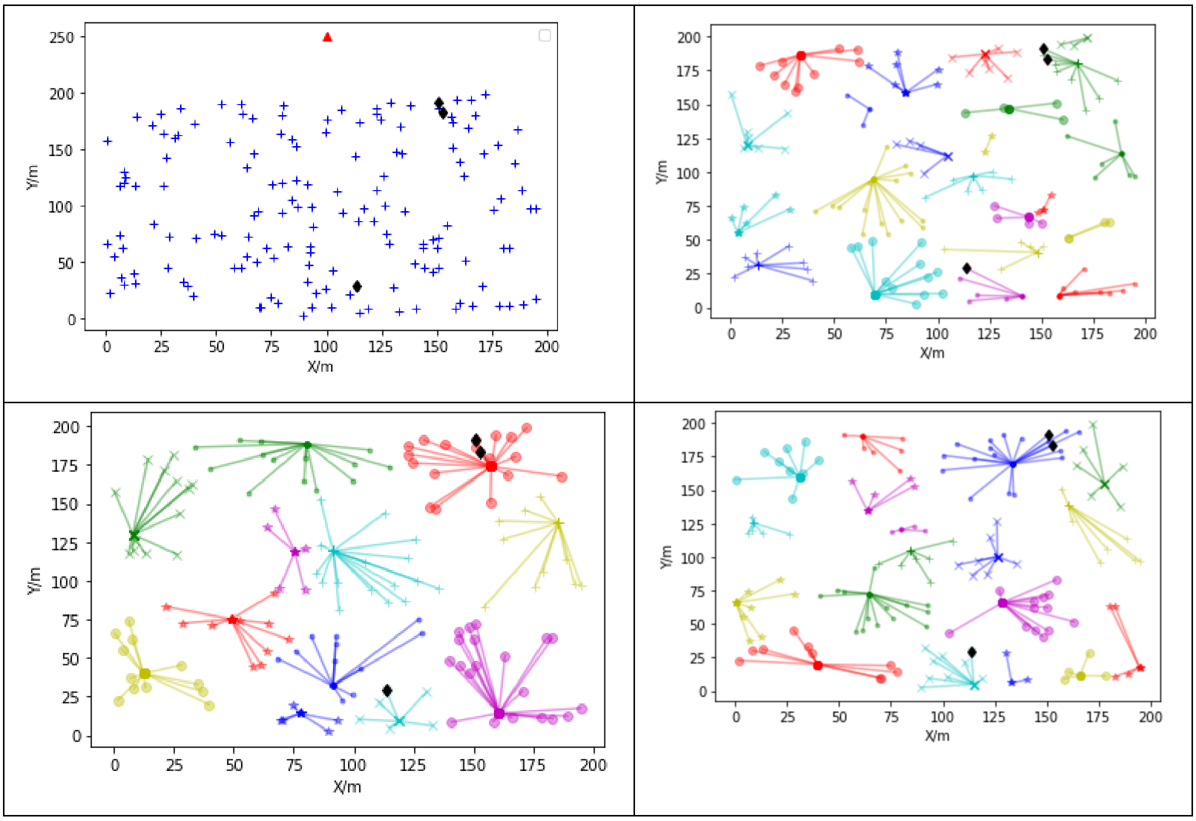

Figure 1: Various stages in cluster head formation and malicious nodes identification.

5. Conclusion

The effect of major constraints in the design of a routing protocol for MANETs can be reduced to a significant level in this proposed method. From the results, we can see that the BFOA is well-suited for efficient route determination in MANETs. In the first stage of this method, fuzzy clustering is used to determine the cluster heads based on an adaptive trust model that uses direct, indirect and recent trust values. The packets are routed through the cluster heads avoiding the paths involving misbehaving nodes. With the proper settings of the threshold values of the trust, malicious nodes can be effectively identified and those nodes can be dropped while selecting the best path using the BFOA algorithm. This results in reduced loss of packets. The suggested method shows faster convergence toward topological changes in the network. The use of ideal hops by BFOA reduces the delay in the transmission and also reduces energy consumption. Thus, the method proposed with BFOA with an enhanced trust model improves the overall efficiency of the network.

References

1. M. Jabirulla and A. Kumar, "Design and analysis of obstacle, mobility and power aware optimal MANET routing—A review," Solid State Technol., vol. 63, no. 3, pp. 46–55, 2020.

2. S. Mostafavi, V. Hakami, and F. Paydar, "A QoS-assured and mobility aware routing protocol for MANETs," Int. J. Informat. Visualizat., vol. 4, no. 1, pp. 1–9, Feb. 2020.

3. O. Oladayo and A. Ashraf, "A secure and energy-aware routing protocol for optimal routing in mobile wireless sensor networks (MWSNs)," Int. J. Sensors, Wireless Commun. Control, vol. 9, no. 4, pp. 507–520, Sep. 2019.

4. J. M. M. Alves, "Path planning and collision avoidance algorithms for small RPAS," M.S. thesis, Dept. Aerosp. Eng., Tecnico LISBOA, Lisbon, Portugal, 2017.

5. R. M. Chintalapalli and V. R. Ananthula, "M-LionWhale: Multi-objective optimisation model for secure routing in mobile ad-hoc network," IET Commun., vol. 12, pp. 1406–1415, 2018.

6. T. D. Nguyen, J. Y. Khan, and D. T. Ngo, "A distributed energy-harvestingaware routing algorithm for heterogeneous IoT networks,'' IEEE Trans. Green Commun. Netw., vol. 2, no. 4, pp. 1115–1127, Dec. 2018.

7. S. Sarkar and R. Datta, ''Mobility-aware route selection technique for mobile ad hoc networks,'' IET Wireless Sensor Syst., vol. 7, no. 3, pp. 55–64, Jun. 2017.

8. Mallikarjuna and V. C. Patil, ''PUSR: Position update secure routing protocol for MANET,'' Int. J. Intell. Eng. Syst., vol. 14, no. 1, pp. 93–102, Feb. 2021.

9. S. R. Halhalli, S. R. Sugave, and B. N. Jagdale, ''Optimisation driven-based secure routing in MANET using atom whale optimization algorithm,'' Int. J. Commun. Netw. Distrib. Syst., vol. 27, no. 1, p. 77, 2021.

10. V. Alappatt and J. P. P. M., ''Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E,'' Int. J. Comput. Netw. Appl., vol. 8, no. 4, p. 400, Aug. 2021.

11. Vahid Heydari 2012, "A new acknowledgment-based scheme against malicious nodes and collusion attack in MANETs", IEEE 14th International Conference on Communication Technology, pp. 784 – 788.

12. Abdulsalam Basabaa, Tarek Sheltami and Elhadi Shakshuki 2014, "Implementation of A3ACKs Intrusion Detection System under Various Mobility Speeds", Procedia Computer Science, vol.32, pp. 571-578.

13. DaehoKang, Hyung-SinKim, ChangheeJoo and SaewoongBahk 2018, "ORGMA: Reliable opportunistic routing with gradient forwarding for MANETs", Elsevier Journals- Computer Networks, vol.131, pp. 52-64.

14. ParthPatel, RajeshBansode and BhushanNemade 2016, "Performance Evaluation of MANET Network Parameters Using AODV Protocol for HEAACK Enhancement", Elsevier Journals- Procedia Computer Science, vol.79, pp. 932-939.

15. Kamini Maheshwar, S. Veenadhari, "Secure Cluster based Routing Protocol for WSN", 2022 IEEE International Conference on Current Development in Engineering and Technology (CCET), pp.1-6, 2022.

16. Hanbing Xie, Gui Zou, Lin Ma, "A Hierarchical Routing Protocol Based on AODV for Unmanned Aerial Vehicle Swarm Network", 2022 IEEE International Conference on Unmanned Systems (ICUS), pp.1113-1117, 2022.

17. Moaath Alshaikh, Akram Morie, "Development of Multipath Dynamic Address Routing Protocol in MANET to Improve Data Transfer in Poor Infrastructure Environment", 2022 International Conference on Computer Science and Software Engineering (CSASE), pp.368-373, 2022.

18. 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, vol.9, pp.163043-163053, 2021.

19. Uppalapati Srilakshmi, Saleh Ahmed Alghamdi, Veera Ankalu Vuyyuru, Neenavath Veeraiah, Youseef Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks", IEEE Access, vol.10, pp.14260-14269, 2022.

20. Samreen Banu Kazi and Mohammed Azharuddin Adhoni "Secure IDS to detect malevolent node in MANETs" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), India, pp. 1363 – 1368, March-2016

21. Rasika R. Mali and Sudhir T. Bagade "Detection of Misbehaving node using Secure Acknowledgement in MANET" International Conference on Computing, Analytics and Security Trends (CAST), India, pp. 611 - 616, December-2016.