Ant Colony Optimization and Trust-based Routing in Mobile Adhoc Network

Ali Abbas

College of Information Technology, Al-Furat Al-Awsat Technical University, Technical Institute, Samawa, Iraq; ali.abbas.isa@atu.edu.iq.

Abstract:

Mobile Adhoc Network (MANETs) consists of dynamicity of the nodes so that multiple routing constraints are required to obtain effective communication among the nodes. Due to the mobility of the nodes, some of the drawbacks occurred in the network such as delay and packet loss. To overcome such drawbacks optimal path selection among the devices and effective routing is essential to attend high quality in communication. For that purpose in this article ant colony optimization and a trust based routing (ACO-TRM) is developed.

Index Terms: Mobile Adhoc Network (MANETs

1 Introduction

MANETs technology becomes most tending nowadays and it occupies maximum of the attention of researchers which are in both the industrial and academic sectors [1-4]. The recent advancement in the design and implementation of routing models which are present in the mobile communication becomes highly efficient and at the time of data transmission it minimizes the loss of packets and power utilization among the nodes in the network [5-8]. The devices which are present in the network perform data transmission in both single hope and multi hope manner [9-12]. The energy of the node which is utilized for did a transmission is very minimal in the beginning stage of the data transmission [13-15].

During fast data transmission the consumption of energy is increased because of multi hope communication [16-20] and improper path selection at the time of data transfer [21-24]. Due to this issue the average delay of the network is increased and the power utilization among the devices is also increased which directly affects the performance of the vehicles which are present in the mobile communication [25-29]. In order to overcome such drawbacks in earlier days effective routing and optimization is concentrated but still it needs improvement to attend maximum efficiency [30-33]. To improve the device mobility [34-37] and dynamic vehicle handling [38-40] with effective path selection in this article and colony optimization and trust based routing is concentrated so that the path connection and vehicle mobility based issues can be neglected and this provides the way to minimize the utilization of energy of any devices which are present in the mobile communication.

2. Related Works:

In [41] author enables dynamic communication in unstable environments in MANET by posing trust management challenges, a blockchain-based reputation model prototype enhances trust management with the disadvantages og high delay. In [42], operates without infrastructure in manet relying on node cooperation for packet transfer by addressing the challenge of malicious nodes to detect On-Off attacks and enhance detection rates and packet delivery and produces high power consumption. In [43], a lightweight trust inference framework for mobile ad hoc networks, emphasizing trust assessment and prediction for the enhancement of ODMRP, supported by convincing experimental results. In [44], explained an Whale Optimization framework using ranking based method which is proposed to enhance IoT network performance by optimizing route establishment, security, and energy consumption with the high overhead. In [45] demonstarted the essential for safety applications in vehicles are gaining popularity for their connectivity with various services ensuring user safety and privacy is crucial for effective safety systems with the high power consumption.

In [46], proposed a fuzzy logic-based control system for a robot taht effectively converting fuzzy range into velocity demonstrating efficient navigation and obstacle avoidance without collisions and the downside is high delay. In [47], developed a novel RPL-based routing protocol using reinforcement learning to enhance IoT network performance in heterogeneous traffic by optimizing queue management and ensuring better QoS and the demerit here is high overhead. In [48], explains the Crow Search-based QoS algorithm (CSA) enhances the QoS in MANETs specifically in AODV routing protocols by improving delay and energy-aware routing and the disadvantage is high power consumption.

In [49], explores the challenges and opportunities of green communication in the smart grid through addressing environmental concerns and reducing CO2 emissions, and high delay is a drawback. In [50], suggested TBSRPM, a "Trust-Based Secure Routing Protocol for MANETs" prioritizing stability and trust in route selection by extending the AODV protocol and enhancing security through Trust Value (TV) and Level of Trust (LOT) and found high power consumption is a drawback. In [51], suggests a cross-layered PSO-based routing protocol for MANETs which integrating trust considerations a dual authentications and enhanced security measures for efficient and secure communication and the demerit here is high overhead. In [52], explained SN-TOCRP, a MANET routing protocol an efficient node with Fuzzy-based Crow Search Algorithm and BTRP ensuring high performance with 96% Packet Delivery Ratio with high energy consumption. In [53], demonstrated ML-AODV, a "Machine Learning and Trust-Based AODV Routing Protocol" for secure MANETs that selects cooperative nodes based on trust metrics and mitigates attacks also improves network performance, but with high power consumption. The earlier model analysis with its merits and demerits are discussed in table 1.

3. Proposed ACO-TRM Model:

This ACO-TRM is mainly designed to provide effective optimization and trust management among the mobile devices which assistances to increase the overall enactment of the mobile communication. The models which are present in this method are ant colony optimization model and trust based routing process. The workflow of the ACO-TRM is shown in figure 1.

3.1 Ant Colony Optimization Model:

In the path discovery phase of an ACO, Forward Ant (FANT) and Backward Ant (BANT) produce new routes. The term "FANT" refers to an element that generates the pheromone route to the initial nodes. Conversely, the BANT creates the pheromone trail for the final node. A unique number for each sequence is printed on the tiny package known as the FANT. Nodes can distinguish duplicate packets rapidly because to sequences and the FANT origin address. The destination node's route must be found and a connection must be made by the source node before it can transmit a packet. Next, the FANT will start to arrive to its one-hop neighbors. If the neighbors are unable to locate the destination, they will continue to forward the

3.2 Trust-based Routing:

Considered to be the most significant assault against the MANET is the warm hole exploit. To pass the data packets in this scenario, the mischievous nodes form a chain. This chain impacts the information packets' entire transmission and manifests as the route leading to the destination. Initially, the network's trust management is part of the implementation. The suggested approach selects a path via the network using trust management. The neighbor node's trust is calculated by the packet delivery ratio. A few bogus packets are transmitted in order to determine the nodes' level of trust. Additionally, those data packets are examined for packet dropping. Our suggested approach addresses energy conservation by giving the network a high level of security. Multiple path routing techniques are employed in conjunction with the trust-based framework to accomplish these goals.

Here's how the algorithm functions:

To determine the nodes' trust, utilize this mechanism.

5. The data packets are transmitted on the trustworthy path following the trust computation.

6. Multipath is employed in the approach that is provided. As soon as the warm hole assaults are identified, the transmission pathways will become available. Additionally, a secure path for communication from the source to the destination will be offered. The idea of several paths is employed so that an alternative way can be used at any point in the event that a path is discovered to be harmful. This leads to an enhancement in the system's performance.

4. Results and Discussion:

Implementation of the proposed and colony optimization and trust based routing model with a suitable for mobile communication is constructed in the ns2 software which is the combination of c++ and object to command language. The optimization methods of incorporated with the network model to obtain better performance and to analyses the results certain parameters are considered they are data success rate, data loss rate, average delay, network throughput and routing overhead. Results of the ACO-TRM model are compared with certain earlier methodologies like SCRPA [51], STOCR [52] and MLTAR [53] and as well the input parameters which are present in this simulation experimentation are given in table 2.

4.1 Data Success Rate: It is the measure of the ratio between the generated data at the source and the receive data in the destination. With the presence of an efficient trust management system the ACO-TRM achieves maximum data success rate and it is shown in the figure 2. From the result it is proven that the ACO-TRM achieves around 6% higher data success rate when compared to other methods like SCRPA, STOCR and MLTAR.

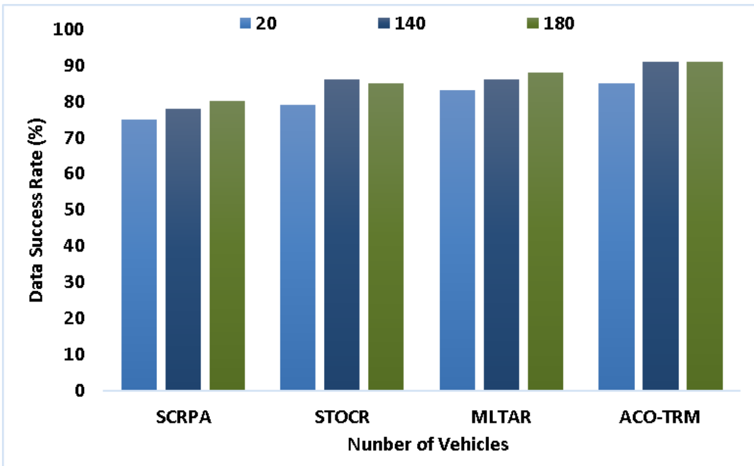

Figure 2 - Data Success Rate

4.2 Data Loss Rate: It is the calculation of the amount of data which gets lost at the time of data transmission among the high speed vehicles. In order to maintain a good standard and communication it becomes very essential to reduce the loss of packets during communication. In figure 3 the data loss rate of the ACO-TRM is illustrated and it is compared with the other works like SCRPA, STOCR and MLTAR. From the time the result is proven that the ACO-TRM produces data loss which is around 25% lower than the other methods.

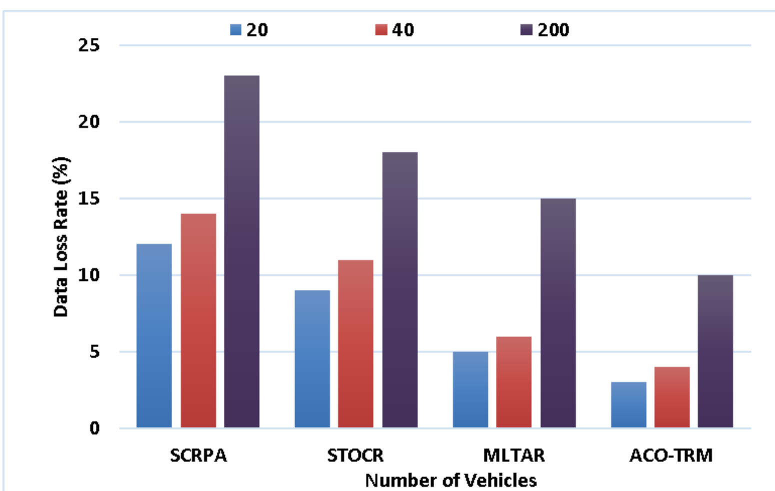

Figure 3 - Data Loss Rate

4.3 Average Delay: It is the calculation of the time difference between the allocated time and the delay time of the transmitted data from the source to the vehicles in the network. To maintain the standard of the communication it is necessary to reduce the delay occurrences among the vehicles. In figure 4 the delay calculation of the ACO-TRM is performed and it is compared with the other methods like SCRPA, STOCR and MLTAR. From this calculation it is proven that the ACO-TRM produces a delay which is around 80 milliseconds lower than the other methods.

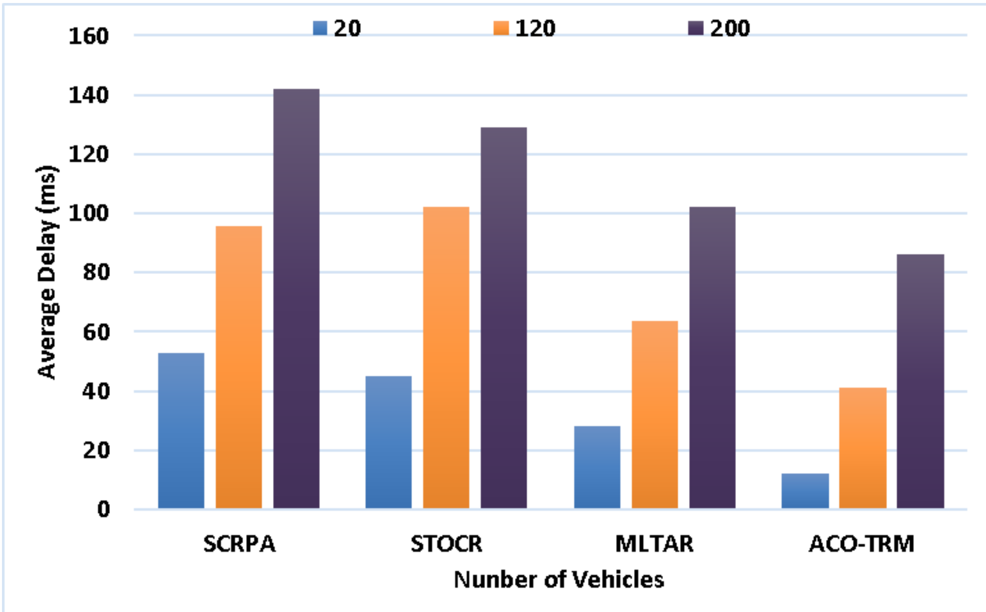

Figure 4 - Average Delay

4.4 Network Throughput: It is the measure of generated packets from the source vehicles which are present in the network. Maximization of throughput directly increases the overall performance and scalability of the network. In figure 5 the throughput calculation is performed for the ACO-TRM and it is compared with the other methods like SCRPA, STOCR and MLTAR.
With the presence of effective optimization model and trust based routing process the throughput level of the ACO-TRM is maximized which is around 70kbps higher than the other methods

4.5 Routing Overhead: It is the calculation of the number of packets which is forwarded back to the source without reaching the destination at the time of data transmission. The count of forwarded data packets is otherwise called routing overhead. In figure 6 the overhead calculation of the ACO-TRM is describe and it is compared with the earlier methods like SCRPA, STOCR and MLTAR. With the presence of effective optimization and trust calculation model the routing overhead of the ACO-TRM is reduced which is around 300 package lower than the earlier methods.

5 Conclusion:
The aim of this proposed ACO-TRM model is to construct optimal path among the devices which are present in the mobile communication and to provide an effective routing model for each data transmission among the devices. For that purpose here ant colony

6. References:

[1] A. H. Abbas, L. Audah, and N. A. M. Alduais, "An Efficient Load Balance Algorithm for Vehicular Ad-Hoc Network," in 2018 Electrical Power, Electronics, Communications

[2] A. H. Abbas, H. Mansour, and A. Al-Fatlawi, "Self-Adaptive Efficient Dynamic Multi-Hop Clustering (SA-EDMC) Approach for Improving VANET's Performance," International

[3] M. A. Jubair, S. A. Mostafa, D. A. Zebari, H. M. Hariz, N. F. Abdulsattar, M. H. Hassan, A. H. Abbas, F. H. Abbas, A. Alasiry, and M. Turki-Hadj, "A QoS Aware Cluster Head Selection and Hybrid

[4] M. I. Habelalmateen, A. J. Ahmed, A. H. Abbas, and S. A. Rashid, "TACRP: Traffic-Aware Clustering-

[5] A. H. Abbas, A. J. Ahmed, S. A. Rashid, M. A. Jubair, N. F. Abdulsattar, H. S. Mansour, and M. I. Habelalmateen, "Hybrid ANT Based Continuous Cuckoo Search Optimization Algorithm for Vehicle

[6] M. I. Habelalmateen, A. H. Abbas, L. Audah, and N. A. M. Alduais, "Dynamic multiagent method to avoid duplicated information at intersections in VANETs," Telkomnika (Teleco

[7] R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas, and A. Alamoody, "An Overview on V2P Communication System: Architecture and Application,

[8] Y.S. Jghef, M.J.M. Jasim, H.M.A. Ghanimi, A.D. Algarni, N.F. Soliman, W. El-Shafai, S.R.M. Zeebaree, A. Alkhayyat, A.S. Abosinnee, N.F. Abdulsattar, A.H. Abbas, H.M. Hariz, and F.H.

[9] G.G. Shayea, D.A. Mohammed, A.H. Abbas, and N.F. Abdulsattar, "Privacy-Aware Secure Routing through Elliptical Curve Cryptography

[10] M.H. Hassan, A.H. Abbas, M.H. Mutar, M.A. Jubair, S.A. Rashid, A.J. Ahmed, M.I. Habelalmateen, A. Mohammed, and L. Audah, "Investigative Study on

[11] N.F. Abdulsattar, F. Abedi, H.M.A. Ghanimi, S. Kumar, A.H. Abbas, A.S. Abosinnee, A. Alkhayyat, M.H. Hassan, and F.H. Abbas, "Botnet Detection Employing a

[12] F. Abedi, S. R. M. Zeebaree, Z. S. Ageed, H. M. A. Ghanimi, A. Alkhayyat, M. A. M. Sadeeq, S. N. Mahmood, A. S. Abosinnee, Z. H. Kareem, A. H. Abbas, W. K. Al-Azzawi, M. M. Jaber, and M. Dauwed, "Sever