An Effective Optimal Path Finding and Trust based Routing Protocol in VANETs Network

Ali Hashim Kazem
*College of Information Technology, Imam Ja'afar Al-Sadiq University, Al-Muthanna 66002, Iraq;*ali.hashem@sadiq.edu.iq.

Abstract

In recent decades several technology sirs introduced in the wireless communication sector and it is evolved to communicate among the vehicles which is termed as Vehicular Ad Hoc Networks (VANETs). Providing intelligent routing among the vehicles which are in huge numbers with random topology becomes the most challenging issue and as well achieving maximum efficiency is very critical. Providing effective routing and intelligent choice of paths between the vehicles during the transfer of data is the fundamental concept of this network. In the vehicular the network, an Efficient Optimum Path Identification and Trust-Based Routing Protocol (EOPTRP) is created for that reason. This technique consists of three sections: trust computation.

Index Terms: Vehicular Ad hoc Networks (VANETs), Robust Optimized Path Finder and Trust-Based Routing Scheme

1 Introduction

Vehicular Ad hoc network (VANETs) [1] is one among the intelligent transportation system (ITS) [2] which communicates with the real world through roadside vehicles [3] and infrastructures and it provides data transmission facilities particularly to the vehicles which are not sufficient to perform effective communication [4]. The base station and the roadside units are located to perform efficient vehicular communication and infrastructure based communication [5]. Additionally, to improve the vehicle safety highly potential vehicles are constructed which provides the way to create an efficient ITS communication [6]. The functional challenges of the vehicles are its high speed and random mobility so that there is always a possibility that there are non-safety constraints [7] and to improve the network of performance it needs to get concentrated [8].

2 Related Works

In [11], Islam Tharwat Abdel-Halim et al., proposed an automobile-based virtual network infrastructure for smart cities that uses moving cars as main communication centers divided into several zones. The entire thing performs better thanks to the architecture. A unique routing system for Urban VANET, targeted at non-safety applications—namely, multiplayer gaming amongst drivers and passengers from various parking lots—was presented by Bhoi et al. in [12]. To guarantee fluid gaming, this method places a high priority on lowering end-to-end latency. The DRL-driven RIS-assisted energy-efficient task offloading strategy in 6G VANETs was suggested by Muhammad Ayzed Mirza et al. in [13]. It makes use of an integrated power management offloading system, utilizing binary and partial offloading. In [14], Sami Abduljabbar Rashid et al., examined VANETs, a subset of MANETs focusing on enhancing road safety and QoS. It also presented a comprehensive review structured into QoS overview, challenges affecting QoS, and a review of data dissemination. In [15], Sami Abduljabbar Rashid et al., introduced a novel methodology for VANETs by proposing a prediction-based multi-hop clustering approach. Enhancing connection stability, energy efficiency, network longevity, and data consolidation are the main goals here.

In [16], Ali Hashim Abbas et al., introduced a novel MAC/NET with Updated Genetic Algorithm which is a Cross Layer Approach for VANETs. The use of an updated Genetic Algorithm ensures optimal path selection. In [17], SAMI ABDULJABBAR RASHID et al., proposed a novel framework for VANET routing. This integrates a VANET system simulation, reliability and a routing algorithm. It also incorporates an optimization block using Enhanced Gaussian Mutation Harmony Searching. In [18], MUSTAFA MAAD HAMDI et al., introduced an Adaptive Jumping Multi-Objective Firefly Algorithm, a meta-heuristic optimization approach for multi-objective optimization in VANETs. This is combined with a Clustering and Forwarding Mechanism, incorporating clustering, probabilistic forwarding. In [19], Mustafa Maad Hamdi et al., investigates early incident detection in VANETs, addressing specific challenges and outlining the role of a traffic monitoring center. It explores various detection techniques, evaluating their strengths and limitations.

In [20], Mohammed Elaryh et al., proposed an exploration into the performance of Voice over Internet protocol services within VANETs, making use of the Link State Routing Protocol Optimization. The investigation is centered on assessing Qos parameters. Ahmad Mohamad Mezher and colleagues presented a unique game-theoretical method in [21] for a multi metric spatial routing protocol designed specifically for VANETs. The concept of games is used in the research as a theoretical framework for resource allocation analysis and optimization. A unique game-theoretical approach to a multi metric spatial routing protocol for VANETs was presented by Raju K Satyanarayana et al. in [22]. This protocol focuses on forwarding video-reporting messages. The advantage and the disadvantages of the earlier researches are given in table 1.

3. Proposed EOPTRP Model:

The primary goals of the EOPTRP concept are to identify the best route for each vehicle and to offer a reliable routing procedure that maximizes vehicle economy. The packet-based forwarding tracking manipulate, trust calculation, and optimum path selection procedure are the three main components of the suggested model. Figure 1 describes the EOPTRP's work flow.

3.1 Optimal Path Selection Process

The quickest route is the one that takes you from the starting point node to the target node. This is because most current automobiles are supplied with computerized maps that indicate the exact locations of streets and crossroads. This route is selected by using the roadway map data of the city and accounting for the quantity of cars on the way. All of the junctions (also known as anchor points) that a packet must pass through in order to get to its destination are included in the optimum path. The endpoint's location (which, in our version, is received via the simulator) is ascertained by a source node S using a localization service prior to transmitting a data packet P to the destinations D. Based on the city's street map data and the number of cars on it, the source node S calculates the set of junctions that the packet must pass through to get to its destination. This group of anchor points is inserted into the packet header by the source node. The source node calculates the optimum route for reaching the destination by calculating the shortest physical path between its position and the destination's location, taking the amount of traffic into consideration. As a result, the only junctions that must be crossed by the data packets in order to go to their destination are included in this ideal path. The following equation yields the optimal:

3.2 Packet Forward Counting Process

We propose a relay-node-centered monitoring scheme to guarantee packet forwarding security during communication. We utilize Figure 1 to provide a quick explanation of this technique. The hash value for each data packet—also referred to as the digital digest—is created using a hashing algorithm prior to transmission and is joined to the package. This ensures the confidentiality and unchangeability of the data packets. while they are being sent. Additionally, the proper relay node forwarding is necessary for the data packet to be sent when the source node uses multi-hop routing to interact with RSU. Consequently, the route's nodes and their reliable neighbors form a cluster. Relay nodes that receive packets with digital digests during multi-hop routing verify that the packets' digital digests are accurate. To the next relaying network behind it, this relay node forwards the packet. if it is accurate. At this point, the packet's digital digest and origin are noted by the relay node's neighbor nodes, who then forward it once again. This digital digest is likewise recorded by the neighbor node's neighbors, but it is not sent.

3.3 Trust Calculation

3.2.1. Current trust

We shall be provided with the node in the set's digest records regarding its neighbors by the suggested packet monitoring and forwarding technique. The ratio of this digest record to the entire digest string determines how trustworthy this node is judged to be by its neighbor. Think about the two cars that are listed below: A and B. Locate the digest string's beginning and conclusion digests, then determine the proportion of accurate digests. In that case, vehicle A's trust assessment for vehicle B is R_{AB}.

In cases when $\sum_{i=1}^{m} R_{iB}$. The B vehicle's trustworthiness assessment is based on the total of its neighbors, or R_{iB}. Here, "m" is the number of vehicles that neighbor car B. This gives us access to the most recent trust values for each node within this communication's range.

3.2.2. Accumulating trust

After determining the vehicular node's trust value as of just now, the RSU adjusts its calculations and gives it an accruing confidence value (T_{Acc}). After an interaction is completed, the participating vehicle nodes have a current trust value, T_{Cur}. When it is contrasted to the trust valueT_{Acc} that the RSU's vehicle nodes are gathering, two scenarios occur

The initial instance:

3.4 Efficient Trust based Routing Protocol

Moreover, launch methods are important to lessen the impact of entering false cars on congestion. This assesses the quantity of disloyal motors by using the drivers. However, this type of dishonesty in the motors may deceive with regard to their haste, which intensifies the traffic at the crossroads. The priority cars display a reliable vehicle in dire need of transportation. Without engaging in any kind of discussion, it may essentially cross the junctions. The cars that are now in use are those that have an urgent need to travel. This discusses the junction passage. It is allowed to cross junctions by traffic. Sections are permitted to cross crossings by the traffic forms after the reliable values have been assessed. The motors with the least amount of urgency are represented by the standardized vehicle. It mostly deals with passage tipping about motor priority. The traffic flow that regulates the high motor vehicle density allows them to be seen. However, low efficiency will be a significant issue when VANETs are heavily maintained by infrastructure, while fully decentralizing the VANET would result in higher overheads. In this sense, VANETs usually connect to a few additional centralized portions of the decentralized portion. Mobile-centered connection

4. Simulation results:

The efficacy of the suggested EOPTRP-UAV network in comparison to the existing technique OLSRP-UAV [20], GTMRP-UAV [21], and BMIML-UAV [22] methods are simulated using the NS2 simulator. The evaluation metrics are Data success rate (%), Data loss rate (%), Average delay (ms), Throughput (kbps) and Routing overhead (pkts). Table 2 provides the elements that are used to build the suggested network model.

4.1 Data Success Rate: Figure 2 measures the data transfer success rate of the EOPTRP-UAV approach and compares it with other ways such as OLSRP-UAV, GTMRP-UAV, and BMIML-UAV. The data delivery ratio is the percentage of successfully delivered data packets among all sent packets.

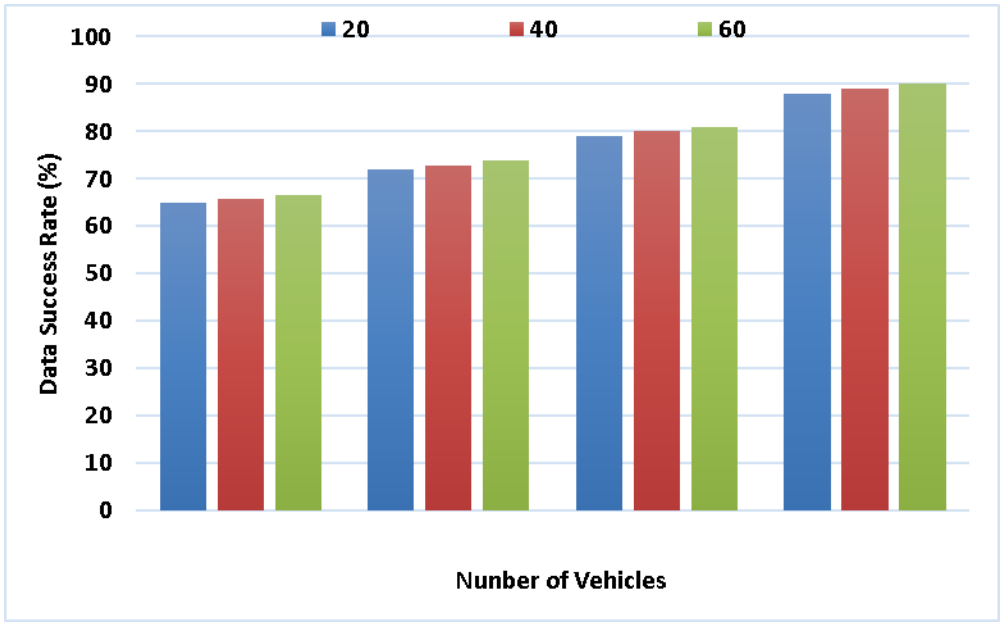

Figure 2 - Data Success Rate

The Proposed EOPTRP method outperforms the existing method of OLSRP at 73%, GTMRP at 80%, and BMIML at 88%, with a high Data Success Rate of 98%. These results indicate that the EOPTRP method has proposed is efficient flawless data transmission.

4.2 Data Loss Rate: It is the ratio of data packets or transmissions that are not successfully reach the destination during the transmission process. In figure 3, the data loss rate of the EOPTRP-UAV method is measured and It is contrasted with alternative techniques such as BMIML-UAV, GTMRP-UAV, and OLSRP-UAV.

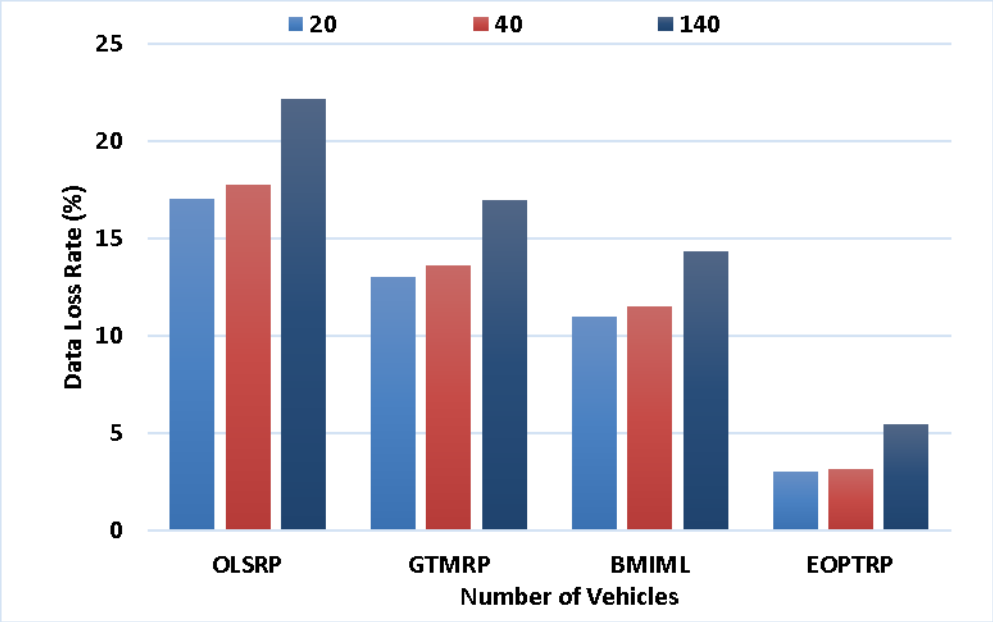

Figure 3 - Data Loss Rate

In comparison to the existing technique of OLSRP at 26%, GTMRP at 19%, and BMIML at 16%, the Proposed EOPTRP obtains a low Data Loss Rate of 9%. This result indicates that the proposed technique is efficient in data transmission.

4.3 Average Delay: The length of time it takes for data packets to go from their source to their destination throughout a network is known as the average delay. Figure 4 shows the measurement of the EOPTRP-UAV method's delay in comparison to other techniques, such as OLSRP-UAV, GTMRP-UAV, and BMIML-UAV.

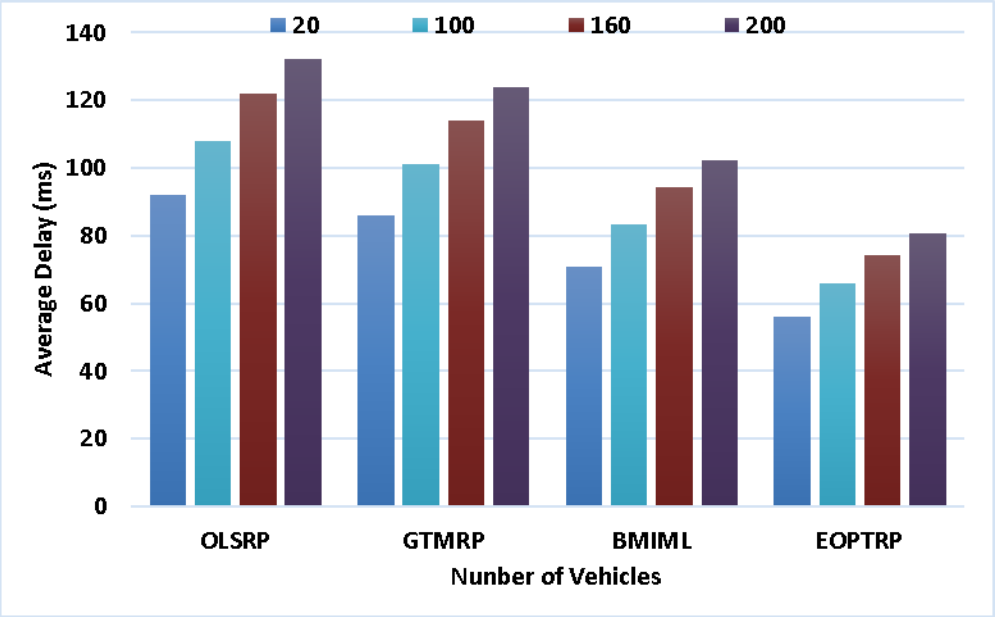

Figure 4 - Average Delay

The Average Delay of the Proposed EOPTRP technique is 81 ms, which is less than the existing technique of OLSRP at 132 ms, GTMRP at 124 ms, and BMIML at 102 ms. In the Proposed EOPTRP technique, a minimum delay indicates fast data transmission.

4.4 Network Throughput: The rate of speed at which data is effectively sent across a communication connection is known as throughput. In figure 5, through put of the EOPTRP-UAV method is measured and it is contrasted with alternative techniques such as BMIML-UAV, GTMRP-UAV, and OLSRP-UAV.

In comparison to the existing technique of OLSRP at 189 kbps, GTMRP at 254 kbps, and BMIML at 296 kbps, the proposed EOPTRP achieves a higher throughput of 402 kbps. This result reveals that a higher data volume may be handled by the proposed EOPTRP approach efficiently.

4.5 Routing Overhead: It refers the extra data packets needed for routing information in a network. Figure 6 shows the measurement and comparison of the routing overhead of the EOPTRP-UAV approach with that of other techniques such as OLSRP-UAV, GTMRP-UAV, and BMIML-UAV.

When compared to the existing technique of OLSRP at 445 packets, GTMRP at 411 packets, and BMIML at 337 packets, the proposed EOPTRP has a minimum routing overhead of 180 packets. This result indicates that the proposed method is efficient in data transmission and throughput generation and as well the final results are given in table 3.

6 References

1. S. Alani, A. Baseel, M.M. Hamdi, and S.A. Rashid, "A hybrid technique for single-source shortest path-based on A* algorithm and ant colony optimization
2. Mohammed, Noor Sabah, et al. "Secure Smart Contract Based on Blockchain to Prevent the Non-Repudiation
3. N. M. Alfahad, S. A. Aliesawi, and F. S. Mubarek, "Enhancing AODV routing protocol based on direction and velocity for real-time urban scenario,"
4. Aliesawi, Salah, Mohammed Ahmed, and Ahmed Rashid. "Iterative multipacket detection with FDE based MAC protocol in vehicular ad hoc networks."

5. M. H. Wasmi, S. A. Aliesawi, and W. M. Jasim, "Distributed semi-clustering protocol for large-scale wireless sensor networks," International J
6. H. Mahdi, B. Al-Bander, M. H. Alwan, M. S. Abood, and M. M. Hamdi, "Vehicular Networks Performance Evaluation Based on Downlink Scheduling Algorithms for High-Speed Long Term Evolution--Vehicle," International Journal o
7. M. M. Hamdi, L. Audah, S. A. Rashid, M. S. Abood, A. S. Mustafa, and M. S. Noori, "A hybrid Algorithms to Improve the Quality of S
8. S. A. Rashid, M. M. Hamdi, and S. Alani, "An overview on quality of service and data dissemination in VANETs," in 2020 International Congress on Human-
9. M.M. Hamdi, L. Audah, and S.A. Rashid, "Data dissemination in VANETs using clustering and probabilistic forwarding based on adaptive jumping multi
10. H.F. Mahdi, M.S. Abood, and M.M. Hamdi, "Performance evaluation for vehicular ad-hoc networks based routing protocols,"
11. I.T. Abdel-Halim and H.M.A. Fahmy, "Toward efficient vehicular-based virtual network infrastructure for smart cities," Engineering Science and Technology, an International Journal, vol. 44, 2023, pp. 101456, doi: 10.1016/j.jestch.2023.101456.
12. S.K. Bhoi, P.M. Khilar, M. Singh, R.R. Sahoo, and R.R. Swain, "A routing protocol for urban vehicular ad hoc networks to support non-safety applications
13. M.A. Mirza, J. Yu, M. Ahmed, S. Raza, W.U. Khan, F. Xu, and A. Nauman, "DRL-driven zero-RIS assisted energy-efficient task