V-Gmir: Geographic Multipath Interference-Resilient Routing For Inter-Path Interference in Vehicular Ad-Hoc Networks

R.Hemalatha[1], R. Amutha[2], R. Deepa[3], P. Prabhakaran[4]

[1]Assistant Professor, Department of B.Voc Networking and Mobile Application, PSG College of Arts & Science, Coimbatore
[2]Associate Professor, Department of Computer Science, PSG College of Arts & Science, Coimbatore
[3]Associate Professor, Department of Information Technology, PSG College of Arts & Science, Coimbatore
[4]Assistant Professor, Department of Information Technology, PSG College of Arts & Science, Coimbatore

Received: 10.07.2024 Revised: 12.08.2024 Accepted: 16.09.2024

ABSTRACT
Particularly with the difficulties presented by dynamic topology and rigorous quality-of- service (QoS) criteria, Vehicular Ad-Hoc Networks (VANETs) depend on strong routing techniques to satisfy the high expectations of current vehicle applications. One practical way to guarantee dependable communication in VANETs is via cross-layer multipath routing. But because wireless communication is broadcast, inter-path interference may seriously reduce performance, therefore impacting many paths concurrently. Furthermore complicating routing in VANETs are low-power wireless communications' unreliability, asymmetry, and error-prone character. In this work, we offer a new routing technique intended to solve inter-path interference in VANETs: V-GMIR (VANET Geographic Multipath Interference-Resilient Routing). Along with a neighbor identification system, the V-GMIR protocol consists on a route finding module with improved RRQ and RRP algorithms. This multi-layer system chooses forwarding nodes based on geographic distance, vehicle speed, and connection quality measurements, therefore lowering interference across closely located paths. V-GMIR provides a more effective answer to the Hidden Node Problem (HNP) at the sink node than conventional protocols, therefore removing the necessity for RTS/CTS handshakes. V-GMIR improves general network dependability and performance by maximizing route selection and guaranteeing reliable connection quality estimations, therefore offering a potential solution for next-generation vehicle communication systems.

Keywords: Geographic Multipath Routing, Hidden Node Problem, Inter-Path Interference, Neighbor Identification, Vanet

1. INTRODUCTION

Modern intelligent transportation systems depend critically on Vehicular Ad-Hoc Networks (VANETs), which let cars interact with one other and with roadside infrastructure to improve road safety, traffic management, and general driving experience [1]. Designed especially for vehicle contexts, VANETs—a subtype of Mobile Ad-Hoc Networks (MANETs)—have automobiles as nodes in a network, hence creating dynamic and self-organizing networks [2]. Supporting many uses including accident prevention, traffic monitoring, entertainment services, and real-time navigation is VANETs main objective [3-4]. To enable fast data interchange between cars and infrastructure, these networks make use of short-range communication technologies as Cellular Vehicle-to- Everything (C-V2X) and Dedicated Short-Range Communications (DSRC [5-6]. Managing the high mobility and fast changing network topology resulting from vehicles driving at different speeds is one of the main difficulties in VANETs [7–9]. Maintaining solid and effective communication relationships becomes challenging in these changing surroundings. To satisfy the rigorous quality-of- service (QoS) criteria for safety-critical applications, VANETs also have to solve problems with routing, interference, and latency [10–11].

Designed to improve communication efficiency in VANETs [12], V-GMIR (Geographic Multipath Interference-Resilient Routing) is a new routing technique. Minimizing inter-path interference—a typical problem in wireless networks where overlapping communication pathways may decrease performance—V-GMIR focuses on addressing the issues presented by dynamic vehicle motions and high mobility [13-14]. V-GMIR maximizes route selection, lowers interference, and guarantees steady data transmission by using geographic routing and multipath techniques, thereby boosting general network dependability and performance for contemporary vehicle applications [15].

This paper is organized as follows for the rest of it. In Section 2, a number of writers discuss several mapping algorithms that are robust to geographic multipath interference. Section 3 displays the V-GMIR model. The findings of the study are reviewed in Section 4. Discussion of the outcome and plans for further research constitute Section 5's last section.

1.1 Motivation of the paper

The rapid growth of intelligent transportation systems and modern vehicular applications places stringent demands on Vehicular Ad-Hoc Networks (VANETs), requiring efficient, high-performance routing protocols capable of handling dynamic topologies and ensuring consistent quality of service (QoS). Traditional routing methods face significant challenges due to inter-path interference, unreliable wireless communication, and the Hidden Node Problem (HNP), which can severely affect network performance. To address these issues, there is a pressing need for an interference-resilient routing protocol that can optimize communication paths while maintaining reliability and minimizing signal interference. V-GMIR is proposed as a solution to fill this gap, aiming to enhance the performance of VANETs through geographic-based multipath routing and interference mitigation techniques.

2. Background study

Israr, A. et al. [4] These days, more and more networks rely on wireless mobile technologies to operate. There was a demand for these networks since they outperform wired systems in many important ways. In addition, it can be used in places where wired systems were not utilized. That was how the mobile nodes were able to achieve the capability of being available at all times and in all places. Nodes were movable and move at random during rescue efforts, which was the finest illustration of how this works in daily life. Dealing with this kind of routing was a pain. To sum up, a dependable protocol and an efficient design were necessities.

Kasana, R., & Kumar, S. [6] In order to deal with the ever-changing traffic conditions caused by shadowing and multipath, this study suggested a Reliable Geographic Routing protocol (RGRP). The next forwarding vehicle was selected based on which nearby vehicle has the best chance of receiving data packets. RGRP works on the assumption that the linkages between the sender and recipient vehicles will last as long as possible, while simultaneously taking into account the degree of association with each nearby car.

Muthukrishnan, P. [8] An OGCR protocol that was ideal for VANETs was being suggested. The clustering method was split into two parts. The first part involves using a chaotic ant swarm optimization (CAS) algorithm to build multi-hop clusters. The second part involves selecting CHs based on the metrics of the optimum cluster members. Next, the author diverted data transmission away from unnecessary inter-cluster communication and toward intra-cluster communication, drawing inspiration from the protocol ant colony system, and last, the author used a mimic differential search (DS) method to eliminate undesired inter-cluster communication.

Qureshi, K. et al. [10] the author looked into the problems with current routing protocols and came up with a VANET routing protocol that was efficient, reliable, and resilient. Problems with connection, latency, reduced throughput, packet loss, and delivery have plagued current routing methods in metropolitan regions because of unpredictable topologies, high node mobility, and network dynamics. In response to these constraints, ISR was developed using distance, traffic density, and node direction for next forwarder and route selection. The author evaluated the performance of ISR to that of other routing protocols by simulating it in a network simulator.

Wahid, I. et al. [13] Research into VANET routing protocols reveals that, in addition to design approach, scenario-based routing was another way to classify VANET routing systems. This classification not only adds another angle from which to examine the routing protocols of VANETs, but it also shows that various situations call for different kinds of routing. Given these facts, the author has created a new taxonomy for VANET routing systems so that young researchers can easily examine them in their own field. The research does not go beyond the standard routing systems, however, which was a drawback.

Zhu, L. et al. [15] The geographical routing protocol for the multilevel VANET has been examined in this study. Through a stochastic analysis and an outside transmission experiment, the author has uncovered the effects of the multilevel structure. According to the results, there was a significant drop in the interlevel communication range of the wireless transmission.

2.1 Problem definition

In VANETs, routing is challenged by dynamic network topologies, high mobility, and strict QoS requirements. The broadcast nature of wireless communication introduces significant inter-path interference, which degrades performance by affecting multiple routes simultaneously. Additionally, issues such as unreliable connections, asymmetry, and the Hidden Node Problem (HNP) further

complicate routing efficiency. Thus, there is a need for an advanced routing protocol that effectively addresses these challenges by minimizing interference and ensuring stable communication in VANETs.

3. MATERIALS AND METHODS

To address the issue of inter-path interference in vanet, V-GMIR, a cross-layer multipath routing protocol, is introduced. Video streaming via vanet must adhere to stringent Quality of Service (QoS) standards, which necessitates effective routing algorithms. Since a wireless channel is basically a broadcast, interference from other pathways has compromise wireless mesh networks.

3.1 System Model

In this part, the suggested protocol's power consumption model and network architecture are described.

3.2 Neighbor Discovery Algorithm

Once the discovery message is received, every node in the listening state will have discovered one neighbor. Unfortunately, the sending node has no way of knowing if its neighbors have really received the data it supplied. If Omni-directional antennas are employed, the positions of the systems neighbor enough to pinpoint its exact location. However, if directional antennas are used, the receiver and the transmitter will need to be in sync with each other to ensure proper antenna steering. When two nodes meet for the first time, this research should arrange another meeting time. The receivers must take part in this procedure, which culminates in a handshake. Here, this research uses two-way techniques of analysis.
Before each time period begins, each node decides whether it will be a transmitter or a receiver. During the first mini slot of a synchronous time slot, if a node is transmitting, it will continue to do so until the conclusion of the slot. In the second mini-slot, this node will proactively search for data that is flowing in the same direction. The first micro slot might be used to route adverts to a certain node in a particular direction. The advertising node must already be a neighbor for the node to decide if it has get advice data; otherwise, it will check. In the second little space, a following advertising node will confirm receipt of its own acknowledgment. In light of this information, the intended parties have chosen to schedule follow-up discussions. In the absence of a "two-way handshake," two nodes will never be able to locate one another.

$$P_{suc_1}(t) = 2_{p_{t1}}.\left(1-p_{t_1}\right).(1-p_{t1})^{M-1}.p_{t1}^{M(t-1)-1} \quad (1)$$

$$P_{suc_2}(t) = 2_{pt_2}\frac{\theta}{2\pi}.(1-p_{t2})\frac{\theta}{2\pi}.\left(1-p_{t2}\frac{\theta}{2\pi}\right)^{M-1}.\left(1-(1-p_{t2})\frac{\theta}{2\pi}\right)^{M-D(t-1)-1} \quad (2)$$

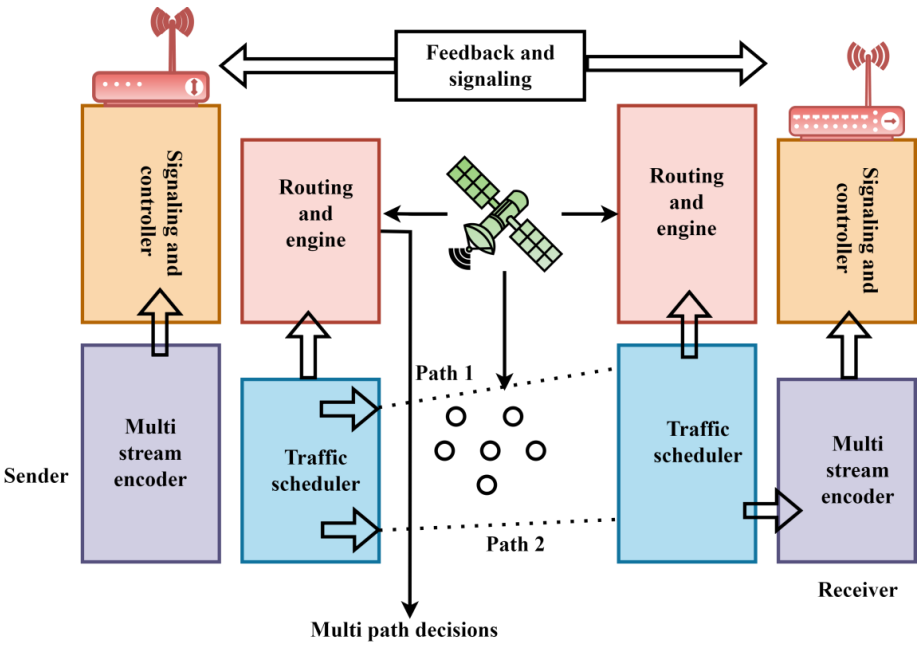

Figure 1: V-GMIR Architecture Diagram

Within a neighbor discovery approach, it is enough for a single successful transmission from a neighbor to reach at least one node. The receiving node will log the identifying information of the sending node in addition to the signal's Angle Of Arrival (AOA) when it receives a strong signal from a passing node. However, if nodes are outfitted with GPS or another finding device for the purpose of determining their

region, then the position data linked with the neighbor is logged. After finding all nearby nodes, the next step is to utilize their positions to send or receive directed transmissions or directional receptions. For future directional transmission or directional reception to neighboring nodes, it is crucial that nodes have location data. However, ND techniques do not impose any requirements on nodes to give this data. Node broadcasting and acknowledgment are assured in ND algorithms.

Algorithm 1: Neighbor Discovery Algorithm

Input:

- Objective state set G
- State space S
- Initial states set I0
- Action space A
- Host number M

Output:

- Attack paths: < R1, R2, R3, ..., Rk >

Algorithmic Steps:

Step 1. Calculate the closure of the objective state set G using Closure(G) algorithm.
Step 2. Assign the result to G+.
Step 3. Extend the graph by adding dense preparation graph using the extendGraph(G, A, M, graph, step, G+) algorithm. Assign the resulting graph to newGraph.
Step 4. Perform a backward search on the newGraph using the backwardSearch(newGraph) algorithm.
Step 5. If the solution is None (indicating no feasible attack path), then:
  a. Update the graph variable to newGraph.
  b. Increment the step variable by 1.
  c. Continue to the next iteration of the loop.
Step 6. If a solution is found, then:
  a. Return the answer (attack path).
  b. Terminate the algorithm.
Step 7. End the if statement.
Step 8. End the while loop.

3.3 Direct Neighbor Discovery Algorithm

Each node in the direct ND algorithm has send data in one way at each time slot with a probability of p_t and listen for incoming data with a probability of p_t. The objective is to determine, given a time constraint, the probabilityp_t that maximizes the discovery rate of new nodes.

Imagine a network of wireless nodes all within transmission range of one another. The node at random has some neighbors. The time period during which a certain station is able to broadcast to a node found using the collision display. When additional stations send data, the node is unable to learn anything from any of them.

$$p_{i,j} = \frac{\theta}{2\pi} p_t \left(1 - \frac{\theta}{2\pi} p_t\right)^{k-2} (1 - p_t) \qquad (3)$$

Whereas stands for the likelihood of transmission at the specified time slot, and beam coverage stands for the likelihood of transmission. Equation (3) defines the likelihood that a node is discovered at a certain instant in time.

$$p_{i,j}(t) = 1 - (1 - p_t)^t \qquad (4)$$

It is focused on increasing the likelihood of a node finding a neighbor within the available window of time in the schedule. In fact, Equation (4) defines any clique finding probability node during the time window. Therefore, each node's ideal is the same.

According to Equation (4), the correct pick is the node with the greatest probability during the specified time range. The value of p_t that should be entered into Equation (4) is the same as the value that is produced by dividing Equation (5).

$$p_t = \frac{\left(2+(k-1)\frac{\theta}{2\pi}\right) - \sqrt{\left(2+(k-1)\frac{\theta}{2\pi}\right)^2 - 4k\frac{\theta}{2\pi}}}{\frac{k\theta}{\pi}} \qquad (5)$$

Its definition in Equation is derived from big (6)

$$p_t = \frac{2\pi}{k\theta} \qquad (6)$$

When nodes are constantly transmitted in a round robin method, the ND probability is naturally employed to its greatest extent. It is beneficial to employ a directional antenna with a limited beam width

because it enables spatial reprocessing. Increasing the proportion of neighbors found is an alternative balance to the one discussed here. Those living nearby might be narrowed down to a chosen few types.
From the wired-in network density, it is easy to determine how many nodes a node is connected to. The equation (7) used to forecast the neighbors of a node.

$$k = \gamma \pi r^2 \qquad (7)$$

Nevertheless, represents the density of WNS nodes per square meter and the network's transmission range. More crashes are likely when the likelihood of gearbox is high. Thus, the channel is gone, along with the opportunity to meet new neighbors, and underestimation.
Similar actions were tracked to inform alternative and. Discovery can be made even if the number of neighbors is estimated incorrectly, and performance declines smoothly as the inaccuracy increases, according to the common belief.
To begin, the investigation presupposed that all nodes are affiliated with exactly one clique. Most networks have a random, multi-hop topology. Second, the actual links that bind the many nodes that makes up the discovery network. The probability of any given node finding another is unrelated to the probability of any given node discovering another. The simulation results used to verify these hypotheses by comparing them to the results obtained from a node's presumed neighbors over time. This research has learned about a node's neighbors using one of the two approaches below.
Therefore, Equation (8) describes the likelihood of discovering the number of neighbors in the initial period.

$$p_i(m,t) = p_i(m-1;t-1)(k-m)p_s + p_i(m;t-1)(k-m-1)p_s] \qquad (8)$$

In contrast, Equation (5.9) defines the likelihood of a successful transmission from a neighboring node to it.

$$p_s = \frac{\theta p_t}{2\pi}\left(1-\frac{\theta p_t}{2\pi}\right)^{k-2}(1-p_t) \qquad (9)$$

Equations (5.10) and (5.11) establish the boundary conditions for the frequent relation.

$$p_i(m,t) = 0, m > t \quad (10)$$

$$p_i(0,0) = 1 \qquad (11)$$

Equation defines the predictable segment of neighbors detected from a node to a point in time(12)

$$F = \frac{\sum_{n=1}^{\min\ (t,k-1)} n p_{\,i}(n,t)}{k-1} \qquad (12)$$

It is challenging to derive an expression from the fraction and then to solve the resulting mathematical equation (10). It determines the value that maximizes the fraction in Equation (11). This makes perfect sense when consider that raising the value in Eq. (12), both the chance of transmission and the chance of discovery rise within a given interval of time. This also increases the expected number of newly identified neighbors spontaneously within the time frame. Equation (12), a comparison of findings for validation purposes, shows the association. In the simulation, each of the one thousand nodes has a 200-meter transmission range and a 10-meter beam width.

3.4 Geographical Routing Protocols

Geographic routing strategies are superior to energy-aware and QoS-aware multipath routing systems for transferring multimedia.
Greedy Perimeter State Routing (GPSR) is one method that uses node locations to determine the path. The GPSR takes use of the nodes' found locations by using positioning technologies like Galileo and GPS. Using the destination node's position as input, the GPSR finds the node along the data delivery route that is geographically nearest to the destination in a greedy approach. The perimeter formation employs the right-hand rule to transmit data packets in situations when gaps prohibit greedy forwarding. Even while GPSR provides superior routing, it does have one limitation: it cannot clear the path to the edge of the map. Furthermore, GPSR will not evaluate new nodes until there is a gap in the energy level and the energy of the closest neighbors has been depleted.
Oblivious Path Vector Face Routing (OPVFR) and the Path Vector Exchange system (PVEX) are two effective local face recognition methods. Unleashing the power of greed Vector Face Routing (GPVFR) enhances routing efficiency by decreasing hop stretch and route stretch — all without identifying the face information or constrained routing state — by recognizing available local face information. Since it depends on committing the locations of faces to memory, the method is power demanding.
Directional Geographical Routing (DGR) was developed as an alternative to GPSR and GPVFR in an effort to fix their aforementioned flaws. With DGR, a video sensor node has deliver many separate but concurrent FEC-protected video streams, which allows for efficient forwarding of real-time video streams. Fewer delays, a longer network life, and higher quality received video are just a few of the benefits of this DGR, which also assists to alleviate route coupling issues. For more eco-friendly data

collection, the DGR adapted for use in green vehicle networks. However, because the high quality of the received video requires a lot of bandwidth, this method cannot accommodate several active video sources. The use of several paths for data transmission causes an energy bottleneck issue for DGR as well. Avoiding problems with user identification at the local level is possible using GOAFR +, an efficient geographical routing strategy. Applying this technique to sensor networks allows for adaptive boundary circle selection—a feature that has lately found extensive application in MANETs—to efficiently choose the border circle, all without requiring any local knowledge of the neighbors' faces. As a result, the routing optimized without increasing the size of the border circle any more than is required. Although this method reduces the expense of forwarding, it cannot accommodate many simultaneously streaming video sources.

While TPGF only finds one shortest route in each iteration, it run several times to identify additional shortest node-disjoint routing pathways as necessary. The first step involves narrowing down the list of viable options to a manageable amount, while the second involves optimizing those options to zero in on the routing route with the fewest feasible stops. With TPGF, it has simultaneously use shortest-path transmission, multipath transmission, and hole-bypassing to get the most out of the network. This study technique, however, falls short when compared to previous work in the geographical advancing stage.

3.5 Route Requests

The method's task pools are initialized with the read request. When the specified time limit or threshold is exceeded, the method organizes requests in the message according to the block ID in order to prevent repetition. It can rebuild the sequence using this way since the hash is stored in the block index. The development of read requests has allowed wasteful one-off queries for specific material to be replaced with more efficient chains of such requests. In addition to reducing the frequency with which the disc must be accessed, the file system's optimization strategy has additional advantages. A hash used to locate read requests that have previously been fulfilled.

$$f(R) = \begin{cases} R_1 * R_2 * R_3 * R_4 * R_5 * R_6 * R_7 = 0, & yes \\ R_1 * R_2 * R_3 * R_4 * R_5 * R_6 * R_7 \quad != 0, & no \end{cases} \qquad (15)$$

Secondly, when S's permutation is non-zero, rebuild the block index by combining duplicate requests according to hash order.

$$PERMUTATION\ S = (R_1 R_2 R_3 R_4 R_5 R_6);\ P_N\ != 0 \qquad (16)$$

Reorder by hash:

$$PERMUTATION\ \ S = \ (R_1 R_2 R_3 R_4 R_5 R_6 R_7);\ P_N\ != 0 \qquad (17)$$

To further enhance the method, duplicate requests across pools are eliminated by modifying the task scheduler during the request identification phase. The procedure then returns to Part A of the algorithm.

3.6 V-GMIR (Geographic Multipath Interference-Resilient Routing)

Deconstructing a network covers the way for doing structural network analysis and encoding problems, both of which assist pinpoint potential entrance points. This means that the outcome of the subnet partition determines the representation used for encoding. The values of this gene include not just the host being targeted, but also all other hosts and vulnerabilities in the same subnet. The range of values for this gene in the host's sub network is determined by the host's vulnerability score. Since there is no correlation between the various kinds of exploitation, this technique encodes them as real numbers.

The address space of the provided host is not occupied by any host on the specified subnet. Since there has only been one host on any given subnet, it is essential to create specialized attacks for each subnet. The gene value range numerically represents the number of operations conducted in each subnet, which in turn displays the size of grounded exploitation activities. The subnet's gene values, for instance, has been anything from zero to mn-1.

Theoretically, the path-finding technique was based on a graph planning method that combines solution searching with graph expansion. The computer will either provide a solution or correctly show that no attack strategy is possible after the compact planning graph is stabilized. The solution that has been extracted is not a simple, all-encompassing plan, but rather a complex system of mechanisms that all work together. The solution thought of as an onion, with each layer representing a different part of the process:

$$(R_1, R_2, \dots, R_K) \qquad (18)$$

By streamlining a multi-layered plan and defining an action-response chain that respects the boundaries of the levels, a comprehensive attack path has been built. An extensive overview of the technique for finding novel attack vectors via the expansion of compact planning graphs is presented in this work.

Algorithm 2: V-GMIR

Input: Encoded vectors E and target host information.
Construct Planning Graph:
Create a compact planning graph based on encoded vectors E and network topology.
Expand the graph considering possible attack paths.
Search for Path:
Use a path finding algorithm to find the optimal attack path that respects subnet boundaries.
Encoding Vulnerabilities:
Input: Subnets $S1 = \{H_1, H_2\}$ with scores [0.1,0.3].
Output: Encoded vector $E_1 = [0.1, 0.3]$
Path Finding:
Input: Encoded vectors E_1, E_2 and target host information.
Output: Attack path (R_1, R_2) or declaration of no path.
Output:
If a solution is found: Return the attack path as a sequence of actions or mechanisms $(R_1, R_2, \ldots, R_K)$
If no solution exists: Return a declaration stating that no feasible attack path was found.

4. Performance Evaluation

This research has evaluated the proposed V-GMIR method in the context of the NS-2 simulation and contrasts it with AMGRP and PGRP. Several characteristics, including as throughput, average latency, energy consumption, number of nodes, and packet delivery ratio, are investigated in the NS-2 simulation environment to evaluate the proposed design.

Table 1. Simulation settings

Parameter	value
Network size	500m x500m
Number of nodes	0-49 nodes
Max Packet	256
Simulation time	300 s
Routing	DSDV
Data link (MAC)	IEEE 802.11
Channel frequency	600KHz
Channel bandwidth	100KHz
Initial energy	20 J
Transmit power	33 dbm
Receive sensitivity	-98 dbm
Receive threshold	-88 dbm
Antenna model	Omni-directional
Maximum transmission range	100 meters

Table 2. Throughput comparison table

Packet Size (bits)	AMGRP	PGRP	V-GMIR
1000	0.125	0.1667	0.25
2000	0.25	0.3333	0.5
3000	0.375	0.5	0.75
4000	0.5	0.6667	1
5000	0.625	0.8333	1.25

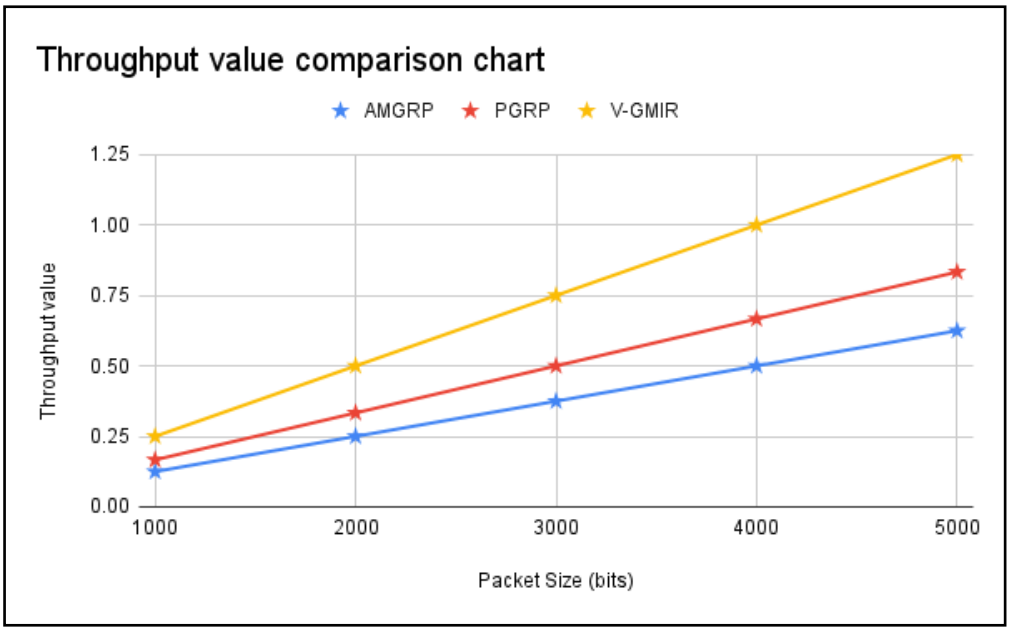

Figure 2: Throughput comparison chart

Three routing protocols—AMGRP, PGRP, and V-GMIR—performance over a range of packet sizes is shown in the table and figure 2. All protocols show gains in performance criteria as packet size rises, which reflects more efficiency with bigger packets. V-GMIR does, however, often beat AMGRP and PGRP all around packet sizes. For example, V-GMIR gets a value of 0.25, which is more than PGRP's 0.1667 and AMGRP's 0.125 at 1000 bits. Increasing packet sizes follow this pattern, where V-GMIR's performance approaches 1.25 at 5000 bits, well above AMGRP's 0.625 and PGRP's 0.8333. This shows that, while processing bigger packets, V-GMIR provides more efficiency and effectiveness than the other protocols, therefore stressing its resilience and capacity in managing rising data loads over them.

Table 3: Energy comparison table

Operating Time (Hrs)	AMGRP	PGRP	V-GMIR
10	4.2	3.8	3
20	8.4	7.6	6
30	12.6	11.4	9
40	16.8	15.2	12
50	21	19	15

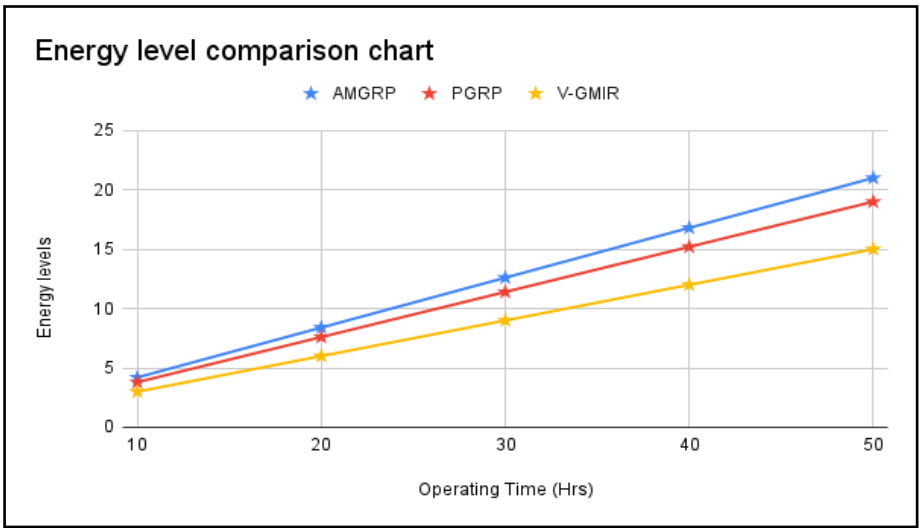

Figure 3: Energy comparison chart

Operating time data shown in Table 3 and Figure 3 indicates the performance of the AMGRP, PGRP, and V-GMIR routing protocols throughout many durations. All procedures exhibit increases in their respective values as the operational time rises, suggesting longer timeframes needed for job completion or processing. V-GMIR shows always better efficiency than AMGRP and PGRP. For instance, V-GMIR notes a value of 3, which is smaller than AMGRP's 4.2 and PGRP's 3.8, thereby suggesting less time needed for operations at 10 hours of operation. As the running duration rises, V-GMIR reaches 15 at 50 hours, compared to AMGRP's 21 and PGRP's 19, therefore preserving this efficiency. These findings imply that V-GMIR not only handles jobs more effectively but also performs better throughout different durations, therefore lowering operating time relative to the other two protocols.

Table 4: Transmission Delay comparison table

Packet Size (bits)	**AMGRP**	**PGRP**	**V-GMIR**
1000	0.016	0.012	0.008
2000	0.032	0.024	0.016
3000	0.048	0.036	0.024
4000	0.064	0.048	0.032
5000	0.08	0.06	0.04

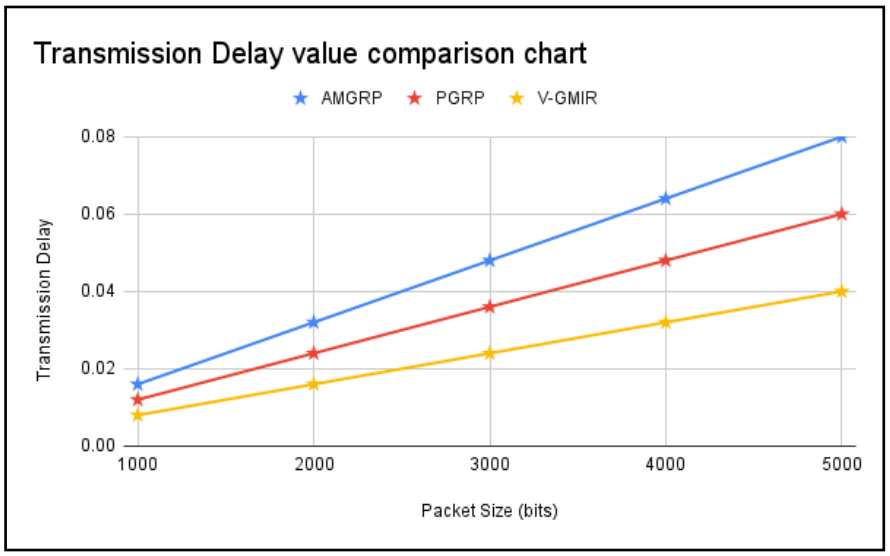

Figure 4: Transmission Delay comparison chart

Table and figure 4 displays transmission delay statistics for the AMGRP, PGRP, and V-GMIR protocols, therefore illuminating how each protocol manages data transfer using different packet sizes. For all protocols, the transmission delay rises as packet size grows to represent the additional time needed to process bigger packets. V-GMIR constantly shows the lowest transmission delay for all packet sizes, thereby demonstrating exceptional performance in delay minimizing. For example, V-GMIR's delay is 0.008 seconds, at 1000 bits, whereas AMGRP's delay is 0.016 seconds and PGRP's delay is 0.012 seconds. Larger packet sizes follow from V-GMIR's delay of 0.04 seconds at 5000 bits whereas AMGRP and PGRP have delays of 0.08 and 0.06 respectively. These findings show V-GMIR's efficiency in lowering transmission time, so handling bigger data packets becomes more profitable than with other protocols.

Table 5: Packet Delivery ratio comparison table

Number of packets	**AMGRP**	**PGRP**	**V-GMIR**
50	96.4	96.6	97.2
100	98.2	98.3	98.6
150	98.8	98.86	99.06
200	99.1	99.15	99.3
250	99.28	99.32	99.44

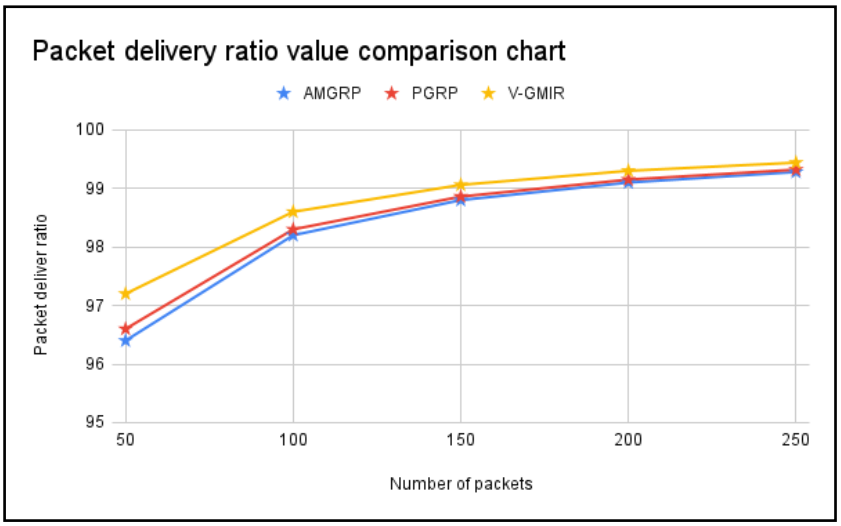

Figure 5: Packet Delivery ratio comparison chart

Data on the amount of packets handled by the AMGRP, PGRP, and V-GMIR protocols indicates in the table and figure five their efficiency in managing packet transmission. All systems demonstrate better performance as the packet count rises and a greater proportion of successful packet transfers. In this measure V-GMIR often beats PGRP and AMGRP. For 50 packets, V-GMIR, for instance, gets a success rate of 97.2%, higher than PGRP's 96.6% and AMGRP's 96.4%. Larger quantities of packets follow this pattern; V-GMIR has a success rate of 99.44% at 250 packets whereas AMGRP's 99.28% and PGRP's 99.32% respectively. These findings show V-GMIR's better capacity to efficiently manage and process packets, therefore guaranteeing a greater rate of successful transmissions than on the other protocols.

5. CONCLUSION

In conclusion, the V-GMIR (Geographic Multipath Interference-Resilient Routing) protocol addresses critical challenges faced by Vehicular Ad-Hoc Networks (VANETs) by introducing a novel approach to managing inter-path interference and optimizing routing performance. By incorporating enhanced RRQ and RRP algorithms, along with a sophisticated neighbor identification technique, V-GMIR effectively mitigates the impact of inter-path interference and overcomes the limitations associated with unreliable and error-prone wireless communication. The elimination of RTS/CTS handshakes and the focus on geographic distance, vehicle speed, and connection quality further enhance the protocol's efficiency and reliability. As a result, V-GMIR provides a robust solution for achieving high-performance routing in VANETs, making it well-suited to meet the demands of modern vehicular applications and contribute to the advancement of next-generation vehicular communication systems.

REFERENCES

[1] Alves Junior, J., & Wille, E. C. (2018). Routing in vehicular ad hoc networks: main characteristics and tendencies. Journal of Computer Networks and Communications, 2018(1), 1302123.
[2] Ghaemi, Y., El-Ocla, H., Yadav, N. R., Madana, M. R., Raju, D. K., Dhanabal, V., & Sheshadri, V. (2021). Intelligent transport system using time delay-based multipath routing protocol for vehicular ad hoc networks. Sensors, 21(22), 7706.
[3] Hiruy, D. (2022). Performance Analysis of Path Selection Routing Protocol based on Geographical Multicast Routing Algorithm for UVANT (Doctoral dissertation)..
[4] Israr, A., Shafiq, M., & Muqeem, S. (2023). Analysis of Greedy Strategies in Geographic Routing of VANETs. Journal of Applied Engineering & Technology (JAET), 7(1), 10-21.
[5] Karimi, R., & Shokrollahi, S. (2018). PGRP: Predictive geographic routing protocol for VANETs. Computer Networks, 141, 67-81.
[6] Kasana, R., & Kumar, S. (2018, March). Reliable geographic routing protocol for vehicular ad-hoc networks under shadowing and multipath environments. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 180-185). IEEE.
[7] Kumari, N. D., & Shylaja, B. S. (2019). AMGRP: AHP-based multimetric geographical routing protocol for urban environment of VANETs. Journal of King Saud University-Computer and Information Sciences, 31(1), 72-81.

[8] Muthukrishnan, P. (2022). Optimal Geographical Cluster Based Routing Protocol in Vehicular Ad-Hoc Networks Using Hybrid Meta-Heuristic Algorithm for Network Lifetime Enhancement. Mathematical Statistician and Engineering Applications, 71(3s2), 1155-1172.

[9] Nebbou, T., Lehsaini, M., & Fouchal, H. (2019). Partial backwards routing protocol for VANETs. Vehicular Communications, 18, 100162.

[10] Qureshi, K. N., Islam, F. U., Kaiwartya, O., Kumar, A., & Lloret, J. (2020). Improved road segment-based geographical routing protocol for vehicular ad-hoc networks. Electronics, 9(8), 1248.

[11] Smiri, S., Boushaba, A., Abbou, R. B., & Zahi, A. (2018, April). Geographic and topology based routing protocols in vehicular ad-hoc networks: Performance evaluation and QoS analysis. In 2018 international conference on intelligent systems and computer vision (IScV) (pp. 1-8). IEEE.

[12] Vafaei, M., Khademzadeh, A., & Pourmina, M. A. (2021). A new QoS adaptive multi-path routing for video streaming in urban VANETs integrating ant colony optimization algorithm and fuzzy logic. Wireless Personal Communications, 118(4), 2539-2572.

[13] Wahid, I., Tanvir, S., Ahmad, M., Ullah, F., AlGhamdi, A. S., Khan, M., & Alshamrani, S. S. (2022). Vehicular Ad Hoc Networks Routing Strategies for Intelligent Transportation System. Electronics, 11(15), 2298.

[14] Zaimi, I., Boushaba, A., Squalli Houssaini, Z., & Oumsis, M. (2019). A fuzzy geographical routing approach to support real-time multimedia transmission for vehicular ad hoc networks. Wireless Networks, 25, 1289-1311.

[15] Zhu, L., Li, C., Li, B., Wang, X., & Mao, G. (2015). Geographic routing in multilevel scenarios of vehicular ad hoc networks. IEEE Transactions on vehicular technology, 65(9), 7740-7753.

[16] Hemalatha, R., & Selvi, S. (2022). Robust collusion avoidance-secure significant VC scheme. *International Journal of Intelligent Engineering & Systems*.

[17] Hemalatha, R., & Selvi, S. (2023). A robust VC scheme for securing cloud data storage. *ARPN Journal of Engineering and Applied Sciences*, 18(4).

[18] Hemalatha, R., & Selvi, S. (2022). Improving security of visual cryptography by contrast sensitivity function. *Vidyabharati International Interdisciplinary Research Journal Science and Technology*.

[19] Hemalatha, R., Selvi, S., & Sathya, R. (2024). Securing cloud data using Hill cipher encoded quick response code and visual cryptography. *Indian Journal of Natural Sciences*, 15(84).