International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 17 (2025) pp. 242–260
© Cerebration Science Publishing

Article

Efficient Route Reliability Algorithm for Vehicular Ad Hoc Networks

Wajid Ali [1], Shalini Z. Ninoria [1], Gulista Khan [2] and Kamal Kumar Gola [3,*]

[1] CCSIT, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh 244001, India; er.wajid.ali@gmail.com
[2] Faculty of Engineering, Teerthanker Mahaveer University, Moradabad, Uttar Pradesh 244001, India; shalinin.computers@tmu.ac.in
[3] College of Smart Computing, COER University, Roorkee, Uttarakhand 247667, India; gulista.khan@gmail.com
* Correspondence author: kkgolaa1503@gmail.com

Received date: 15 July 2024; Accepted date: 5 March 2025; Published online: 27 March 2025

Abstract: To ensure the efficient functioning of intelligent transportation systems, it's crucial to establish reliable communication channels with vehicles and roadside units. Vehicular ad hoc networks (VANETs) offer a brilliant solution for facilitating such communication among vehicles nodes and other units. However, due to the dynamic nature of VANETs characterized by high mobility and frequent topology changes, developing a dependable routing algorithm is a significant challenge. Given the vulnerability of communication links in VANETs to disconnection, ensuring routing reliability is paramount in these dynamic networks. This paper proposed a novel reliable model for VANET aimed at facilitating dependable path finding in VANETs. Central to our approach is the concept of link reliability, which represents the probability of maintaining a continuous operational link of communication among vehicles over a specific duration. We achieve precise computation of link reliability by leveraging vehicle location, velocity, and direction data along roadways. Our proposed dependable routing protocol, AODV-R, builds upon the widely-used ad hoc on-demand distance vector (AODV) routing protocol. Simulation results demonstrate that AODV-R, while reducing routing control overhead, outperforms the standard AODV protocol for enhanced delivery ratio and reduced link failures.

Keywords: VANET; link reliability; AODV; routing reliability

1. Introduction

In recent times, both academic and business communities have acknowledged the potential advantages of promoting collaboration among road transportation system and vehicles. These benefits include enhanced driver safety, improved road efficiency, and reduced environmental impact. Consequently, there has been a surge in focus and investigate efforts directed towards the expansion of VANETs [1]. This aims to facilitate dynamic route routing, emergency message dissemination and, crucially, safe driving [2]. Although VANETs constitute a distinct group of Mobile Ad Hoc Networks (MANETs), they share several key characteristics. Notably, owing to the dynamic movement of VANET network nodes, the network topology undergoes constant fluctuations. As a consequence of vehicle movements and drivers' behaviors, communication links between vehicles experience rapid variations and are susceptible to disconnection. Fortunately, owing to their movement being governed by traffic networks and regulations, predictions can be made while travelling along roads. Moreover, compared to MANETs, VANETs often possess greater communication power and computing capacity.

The unique description of VANETs pose significant routing challenges that must be understood so that networks could be efficiently utilized [3]. Arguably, most challenging issues is the network's high mobility and frequent topology changes [4,5]. As vehicles change lanes or speeds, the topology of vehicular networks may also shift, with these adjustments being instantaneous and dependent on drivers,

Copyright: © 2025 by the authors

traffic patterns, and road conditions. Consequently, routing techniques and protocols proposed for VANETs must adapt rapidly to accommodate these dynamic topology changes. Additionally, they must be well-organized and give Quality-of-Service (QoS) support to allow for varying transmission priorities base on the kind of data flow. Existing routing protocols, designed for MANETs, are ill-suited for VANETs due to their inherent differences.

In this paper, we recommend a novel reliability-based routing system aimed at establishing a more dependable pathway from source and destination nodes. The novelty of our approach lies in the expansion of a routing prototype that considers both connection breakages and the statistical distribution of vehicle movements. Specifically, our work focuses on scenarios involving vehicles travelling in two different directions on roadways at varying velocities. To evaluate the ability of our proposed scheme, we conduct wide simulation study comparing it with the AODV routing protocol. A Reliable AODV protocol enhanced AODV by integrating **trust-based routing, QoS-aware metrics, link stability prediction, load balancing, and optimized route discovery**. These improvements would make AODV more suitable for highly dynamic VANET environments while ensuring **better reliability, security, and performance**. Our evaluation criteria include average end-to-end delay, packet delivery ratio, average number of link failures and routing control overhead.

This paper is structured as follows:

- In the "Related Works" section, we compile existing research in this area.
- The "Background of Vehicular Communications" section provides an overview of the history of vehicle communication technologies.
- We present our suggested vehicle reliability model, including the Proposal of our numerical model to determine link reliability values, in the "Vehicular Reliability Model" section.
- The "AODV-R Reliability-Based Routing Protocol" section elaborates on our AODV-R reliability-based routing protocol.
- We describe the simulation scenario setup and present our findings in the "Simulation Setup and Results" section.
- Finally, we conclude our paper in the "Conclusion" section.

2. Related Work

This section explains the state of art for VANET Communication. It has been categorized in two parts: Mobility based protocols and Prediction based protocols.

2.1. Mobility Based Routing Protocol

Routing reliability predominantly focuses on Mobile Ad Hoc Networks (MANETs), as evidenced by studies such as [6,7]. Taleb and colleagues [8] introduced a scheme tailored for VANETs, leveraging vehicle heading data to pre-empt potential link breakages. Their approach utilizes vehicle velocity vectors to group vehicles, enabling the scheme to seek more stable routes incorporating vehicles within same group should a route involving a vehicle become unstable due to group changes.

In [9], a novel velocity-aided routing procedure for VANETs was planned by researchers. It determines packet forwarding schemes based on the comparative velocity among the relay node and the end node. This algorithm proposes the packet forwarding route by considering the future trajectory and the velocity of the nodes.

In [10] author presents a novel authentication scheme designed to address the security and privacy challenges in 5G-assisted vehicular fog computing environments. The proposed scheme utilizes bilinear pairing-based cryptographic techniques to enable anonymous authentication for vehicles and roadside units, ensuring both secure communication and privacy preservation. By leveraging the decentralized nature of fog computing and the low-latency advantages of 5G, the scheme allows for real-time, efficient authentication of vehicles without exposing their identities. The paper highlights how this approach mitigates potential threats such as identity disclosure and unauthorized access, making it a promising solution for secure vehicular communication and applications in future smart cities and autonomous driving systems.

In [11] author demonstrates that CLA-FC5G effectively mitigates security threats, including unauthorized access and impersonation, while improving scalability and computational efficiency in the dynamic, resource-constrained environment of vehicular networks.

In [12] author demonstrates that the proposed DDoS mitigation technique not only enhances the security of 5G vehicular networks but also improves the network's resilience, ensuring seamless and reliable communication in a highly dynamic and resource-constrained environment.

In [13] author proposed scheme leverages oblivious transfer (OT) techniques to enable secure and privacy-preserving authentication between vehicles, roadside units, and other network entities without

revealing sensitive information. By using OT, the protocol ensures that communication parties can authenticate each other while keeping their private data hidden, thus protecting user privacy in dynamic vehicular networks. Although above s maintains the security of protocol but they did not discuss the reliability of the data communication.

2.2. Prediction Based Protocols

In [14], authors introduced a routing algorithm based on prediction (PBR) protocol specifically designed for the dynamic scenario in VANETs. Leveraging the predictable movement patterns of nodes on highways, PBR anticipates route lifespan and proactively generates novel route previous to the current ones break. Link lifetime estimation is based on factors such as communication range, vehicle locations, and corresponding velocities, with route lifetime determined by the shortest link lifetime along a route.

In [15], the movement prediction-based routing algorithm (MOPR) was proposed, aiming to identify stable paths to prevent link failures by forecasting future vehicle positions. MOPR selects the steadiest route among multiple possibilities connecting generating and end vehicles, considering association situation of intermediary nodes relative to generating and end nodes. Each vehicle's position, direction, and velocity data are utilized in this process, necessitating an extension of each node's routing table to meet algorithmic requirements.

2.3. Related Work of Vehicular Communications

The development of VANETs was primarily driven by the aim to enhance road safety and prevent accidents through the dissemination of secure safety data among vehicles. Depending on specific requirements, information gathered from a vehicle's sensors can be disseminated to nearby vehicles, transmitted to a roadside unit (RSU), or displayed to the driver [16]. Additionally, beyond road safety, VANETs offer a wide array of other potential applications, including Internet connectivity, multimedia and gaming applications, car-to-home communication, and the distribution of travel and tourism information.

The formation of automotive networks can be divided into 3 categories, as illustrated in Figure 1:

- Inter-vehicle communication, it is pure ad hoc networking or vehicle-to-vehicle (V2V) communication, in this category vehicles converse with each other without the support of infrastructure. Important data gathered by a vehicle's sensors or transmitted to vehicle can be shared with nearby vehicles.
- Vehicle-to-infrastructure (V2I) communication, it is also termed as vehicle-to-roadside communication, enables vehicles to connect to the Internet and access vehicular applications using wireless local area network access points and cellular gateways [17].
- Inter-roadside communication, which involves communication between hybrid vehicles and the roadside infrastructure.

Ad hoc or peer-to-peer communication enables vehicles to share the information with other vehicle and other road side entities. These vehicle nodes can communicate other entities directly or through relay nodes. This architecture offers better suppleness in sharing the information and integrates V2V communication effectively.

2.4. The Unique Qualities of VANETs

Similar to MANETs, VANETs exhibit self-organizing capabilities, allowing network nodes to manage information distribution autonomously without relying on an essential authority or server to control communication [18].

Moreover, VANETs offer few benefits over MANETs [19]:

- Greater power of transmission and storage: Generally, VANET nodes possess more communication power and storage space capacity compared to MANET network nodes.
- Greater computational capacity: Operating vehicles in Vehicular Ad hoc Networks can afford greater computing, communication, and capabilities of sensing compared to MANETs.
- Predictable mobility: VANET network nodes travel on a network, enabling their movement to be predicted, unlike in MANETs. With knowledge of road trajectory and current velocity, it becomes feasible to forecast a vehicle's future position.

3. Challenging VANET Routing Requirements

The routing process presents a critical challenge that must be overcome for the successful deployment of VANETs due to their unique characteristics. However, the high dynamics, frequent changes in vehicle

densities, and anticipated large number of vehicles pretence considerable challenges for routing. VANETs often experience partitioning due to crossings, traffic lights, and similar traffic network conditions, further complicating the routing process. Nonetheless, mobility constraints and predictable mobility on roads can be advantageous for designing routing protocols in VANETs. Moreover, leveraging other available data such as geographic coordinates and city maps can enhance routing efficiency. Currently, routing protocols for VANETs can be categorized into five groups [15–27]:

- Mobility-based routing protocols utilize mobility information, including relative distance, velocity, acceleration, and movement directions, to predict the lifetime or duration of routing paths.
- Flooding-based routing protocols simply broadcast messages across the network without specific routing strategies.
- Infrastructure-based routing protocols utilize infrastructure such as Roadside Units (RSUs), cellular base stations, and routine buses to aim prove the security and robustness of VANET communications.
- Geographic based routing protocols enable VANETs to identify routes near to the final vehicle using GPS location coordinates.
- Routing protocols based on Probability describe the probability of specific events, such as link breakage at a given broadcast power or mobility parameter, using probability theory.
- Frequent Route Breakage: AODV relies on dynamically discovered routes, making it highly sensitive to node mobility. Frequent topology changes lead to frequent route failures, increasing end-to-end delay.
- High Routing Overhead: AODV floods the network with route request (RREQ) packets, leading to excessive control overhead, especially in high-density VANET scenarios.
- Lack of Trust and Security: AODV is vulnerable to routing attacks such as black hole, gray hole, and Sybil attacks, as it does not verify the trustworthiness of nodes.
- Route Selection Based Only on Hop Count: AODV selects routes based on the minimum hop count, which may not always ensure high reliability or low latency.
- High End-to-End Delay: Route discovery in AODV introduces delay, as paths are established only when needed, which is inefficient for time-sensitive VANET applications.
- Limited Support for Load Balancing: AODV does not consider traffic load distribution, leading to congestion on frequently used routes.
- Energy Consumption Concerns (in IoT-Enabled VANETs): Although energy constraints are not a primary issue in VANETs, IoT-based VANET nodes may have limited power resources. AODV does not optimize energy usage.

4. Reliable Routing Scheme

This section delineates the network environment and introduces the proposed scheme, which prioritizes establishing reliable paths from source node to destination node. In this scheme, mobile agents are employed to gather various information pertinent to vehicles and manage them intelligently based on this data. Additionally, the proposed scheme aims to alleviate scalability issues. By utilizing a mobile agent-based approach, the scheme effectively controls congestion stemming from heavy bandwidth usage, buffer, and cache memory in VANETs, consequently ensuring an efficient and reliable path among source and destination.

This algorithm enhances traditional routing mechanisms by incorporating additional fields in both route request and route reply packets pertaining to cluster member and cluster head information.

A. Network Environment

The proposed dependable routing scheme is tailored for a VANET setting, illustrated in Fig. 1. Within this context, vehicles, or nodes, are randomly dispersed across the network, each operating within its defined parameters such as transmission range, mobility, buffer memory, cache memory, and bandwidth usage.

When a source node needs to establish communication with a destination node, it relies on one or more intermediary nodes. Nodes within the transmission radius of an exacting node are considered its neighbours. The initiating node, referred as the source node, seeks to converse with another designated node known as the destination node.

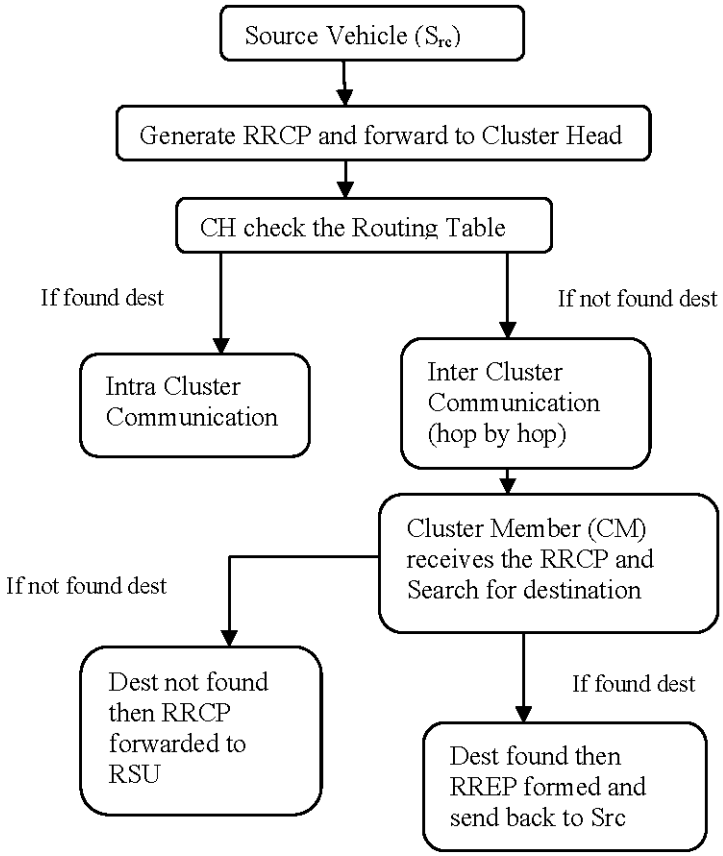

Figure 1. Block diagram of Route finding in AODV-R.

Given the hypothesis that all vehicles equipped with GPS capabilities, their positions, directions, and velocities can be ascertained. To initiate the route establishment process, the source node broadcasts a Route Request (RRCP) Control Packet to all other nodes. This RRCP packet contains essential details such as the source ID, the source's position, and its communication range. Upon reception of the RRCP packet, nodes compute the Euclidean distance between themselves and the source node using Equation (1). If this calculated distance falls within the communication range, indicating proximity, the receiving node responds by transmitting a Route Reply (RREP) Acknowledge Packet back to the source node. Conversely, if the distance exceeds the communication range, the RRCP packet is disregarded. Upon receipt of the RREP packet, the source node proceeds to establish its connection pattern, while all previous nodes in the network follow suit, creating their respective connection patterns.

To ensure optimal network performance in high-density VANETs, the algorithm reduces redundant message exchanges through optimized cluster formation and trust evaluation mechanisms. During the request forwarded phase from hop to hop all the nodes on the route attaches the reliability score of their neighbour nodes along with RRCP message. If any node reliability score is less than threshold (0.6) then this route is discarded. That ensure the reliability of the path. By optimizing computational efficiency, the algorithm maintain low latency, minimal overhead, and high reliability, ensuring smooth communication even in dense traffic conditions. Scalability issue has also been considered and well addressed by taking the clustering approach for data transfer. However in case of high velocity this clustering approach may have some downfalls.

B. Mathematical Model

Let's denote a group of vehicles as G, expressed as:

$$G = \{ V_0, V_1, V_2, ..., V_N\} \quad (1)$$

Here,

- V_0, V_1, V_2 represents the source of the broadcast.
- V_0, V_1, V_2, ..., V_N represent the intermediate nodes among the source and destination.
- V_N signifies the final vehicle that receives the broadcasted information from the source V_0.

We assumed that all vehicles in this scenario maintains the same speed or velocity, measured in kilometres per hour. With this assumption, we can employ the Euclidean Distance formula to compute the distance among two vehicles, whether they are travelling in the in same row regardless of whether they are moving in the same direction or opposite directions.
The formula for Euclidean Distance is expressed as:

$$D_{ij}= \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (2)$$

where:

- (x_1,y_1) represents the location of the first vehicle.
- (x_2,y_2) represents the location of the second vehicle.

Additionally, under the assumption that $D_{ij}>0$ (implying that no two vehicles can have the same location simultaneously with the same speed/velocity), we can calculate the time gap between vehicles as follows:

To calculate gap of between to two vehicles,

$$T_g = D_{ijavg}/Vs \quad (3)$$

Here:

- T_g denotes the time gap.
- D_{ijavg} represents the average distance between two vehicles.
- V_s signifies the average velocity of vehicles.
- l represents a parameter.

To calculate the traffic flow measured, we use the formula:

$$T_f= l/ T_g \quad (4)$$

where:

- T_f signifies the traffic flow measured, i.e., the count of vehicles per second.

In this scenario, it is assumed that all vehicles employ uniform transmission power or energy (measured in joules) and engage in communication within a predefined range (measured in meters). Moreover, the information to be disseminated, such as the size of the information packet, is quantified in kilobytes [20].

To further clarify, we have:

- Transmission power/energy: All vehicles emit signals with the same amount of power or energy, ensuring uniformity in communication capabilities.
- Communication range: Each vehicle can converse with other vehicles within a predefined range, implying that any vehicle beyond this range would not receive the transmitted signal.
- Information packet size: The data to be transmitted, represented by the information packet, is standardized to a specific size, typically measured in kilobytes. This size denotes the amount of information contained in each packet, influencing factors such as transmission time and energy consumption during communication.

These assumptions provide a basis for analyzing communication efficiency, energy consumption, and network performance within the VANET scenario.

C. Cluster Formation in VANET

In VANETs, a cluster refers to a cohesive group of vehicles capable of maintaining uninterrupted communication and identifying themselves as part of the same cluster. In our approach, clusters are established using information such as traffic flow, as well as general vehicle attributes like speed, direction, location, and lane. Each cluster consists of vehicle nodes which are communicated using direct connections with each other. Additionally, neighboring nodes facilitate links between clusters.

When considering routes from a source to a destination, multiple paths may exist. Nodes within any cluster can reach nodes in other clusters via intermediate nodes. This decentralized structure ensures robust communication and facilitates efficient routing within the VANET environment.

a. Cluster Member Update

Cluster member update is an essential process in VANETs, primarily triggered by changes in a vehicle's speed or direction. When a vehicle (V) changes its speed or direction, the Cluster Head (CH) estimates the vehicle's current location based on its previous speed and location data. Consequently, the Cluster Member (CM) update becomes necessary to ensure that the CM's current speed and location are accurately reflected, facilitating seamless data forwarding within the cluster.

b. CH Re-selection

The Cluster Head (CH) assumes a critical role in initiating data communication within VANETs, typically kick starting the process from the source node. It's crucial for the CH to maintain long-term stability within a cluster. Moreover, to ensure the efficiency of the network, the same vehicle (V) cannot serve as CH for an extended period. Hence, CH re-selection becomes necessary to facilitate smooth cluster operation.

The CH re-selection process, involves swiftly identifying and appointing a new CH to maintain cluster stability and ensure uninterrupted data communication. This process must be executed faster than the election of Cluster Member to enable rapid cluster formation and maintain the network's agility.

c. Cluster Merging

Cluster merging offers a robust solution for addressing communication management and reducing unnecessary overhead in VANETs. In scenarios where the Cluster Head (CH) vehicle is distant from Cluster Member (CM) vehicles, CM vehicles may receive a joining message from a nearby CH vehicle, prompting them to join the cluster. However, to further enhance cluster formation and communication effectiveness, clusters may merge when deemed appropriate.

Cluster merging process in the proposed algorithm, showcasing how clusters combine to form more efficient cluster formations and enhance communication within the VANET environment. This process optimizes network resources and improves overall network performance by consolidating clusters and minimizing redundant management overhead.

D. Proposed Algorithm

This section proposed efficient and reliable routing scheme tailored for VANETs. It aims to establish dependable routing paths by considering various parameters of vehicles, including mobility, direction, bandwidth, and congestion. The operational process of the scheme is as follows:

To form reliable paths, the following assumptions are made:

1. The data originating vehicle node (Src) generates a Request Control Packet (RRCP) for route and forwards it to the Cluster Head (CH).
2. If the destination (dest) is listed in the path finding table of the CH, intra-cluster communication is conducted to reach the end mode using the proposed reliable algorithm.
3. If the destination (dest) is not listed in routing table of the CH, inter-cluster communication is processed hop by hop until the Most Reliable Path (MRP) is discovered.
4. Every Cluster Member (CM) receives the Source (Src) vehicle's RRCP message and checks for the destination (dest).
5. If the destination (dest) is found, the discovery process halts, and a Route Reply (RREP) is forwarded backward to reach the Source (Src). If the RRCP is not found, it is forwarded to the Road Side Unit (RSU) to reach the destination (dest).

Pseudo Code of Proposed Algorithm:

```
Function sendRRCP(Src, dest):
   Src generates RRCP and forwards it to CH
   RRCP = generateRRCP(Src, dest)
   forwardToCH(RRCP)

Function forwardToCH(RRCP):
   // Forward RRCP to CH
   CH = findClusterHead()
   sendPacket(RRCP, CH)

Function receiveRRCP(RRCP):
 CM receives RRCP and checks for dest
   if RRCP.dest == myDest:
      sendRREP(RRCP.src, RRCP.dest)
      return
   else if isInPathFindingTable(RRCP.dest):
      //Intra-cluster communication
      intraClusterCommunication (RRCP)
   else:
     // Inter-cluster communication
      interClusterCommunication(RRCP)
```

```
Function intraClusterCommunication(RRCP):
    // Conduct intra-cluster communication to reach dest
    // using proposed reliable algorithm

Function interClusterCommunication(RRCP):
    // Forward RRCP hop by hop until MRP is discovered
    nextHop = getNextHop(RRCP.dest)
    sendPacket(RRCP, nextHop)

Function sendRREP(Src, dest):
    Send Route Reply (RREP) backward to reach Src
    RREP = generateRREP(Src, dest)
    backwardToSrc(RREP)

Function backwardToSrc(RREP):
    // Forward RREP backward to Src
    sendPacket(RREP, Src)

Function generateRRCP(Src, dest):
    // Generate RRCP packet
    RRCP = createPacket(Src, dest)
    return RRCP

Function generateRREP(Src, dest):
    // Generate RREP packet
    RREP = createPacket(Src, dest)
    return RREP

Function findClusterHead():
    // Find the Cluster Head (CH)
    return CH

Function isInPathFindingTable(dest):
    // Check if dest is listed in the path finding table of CH
    // This function will check if the dest is in the table
    return isFound

Function getNextHop(dest):
    // Get the next hop towards dest
    // This function will determine the next hop in the path
    return nextHop

Function sendPacket(packet, destination):
    // Send packet to the destination
    // This function will handle the communication process
    // to send the packet to the specified destination
```

This pseudo code outlines the steps described in the algorithm. It includes functions for generating RRCP and RREP packets, forwarding packets to CH, intra-cluster and inter-cluster communication, finding the next hop, and sending packets.

A detailed algorithmic representation of this process is provided in Figure 1. This algorithm ensures efficient and reliable routing within the VANET environment, considering the dynamic nature of vehicular networks and varying communication conditions.

E. Reliability Analysis of path between two nodes:

Once a reliable path is established between the sources and sink nodes in the VANET network, it becomes essential to verify the reliability of the intermediate nodes along this path. The VANET network can be represented as a graph G, where nodes signify vehicles and edges symbolize communication links between vehicles. To determine the chance of flourishing transmission between two nodes, namely the

source S and the destination D, a model [27] can be employed.

To calculate the chance of flourishing data exchange, a customized version of the Dijkstra algorithm utilized. This algorithm is iteratively executed, with the no. of iterations equal to the no. of paths required between the source S and destination D. During each iteration, the graph G is adjusted to decrease the probability of the path using a multiplying factor known as the decrement factor α.

Through the iterative application of this modified Dijkstra algorithm and the adjustment of the graph G to reflect the decreased probability of each path, the dependability of the intermediate nodes along the established route among the initiated node and destination nodes in the Vehicular Ad hoc network can be assessed. This repeated process ensures that the selected path maintains its reliability even amidst dynamic network conditions.

F. Efficient delivery of data packet from source node to destination node:

To compute the data transmission time from the initiated node to the destination node in a VANET, various factors such as energy expenditure and bandwidth utilization needed to be in consideration.
Let's consider:

- E is the energy required to transmit one packet of data to neighboring vehicles (measured in joules).
- b_{ij} as the bandwidth utilized in packet transmission (measured in bits per second).

We can calculate the data transmission time T_{ij} from the starting place to the target using the following formula:

$$T_{ij} = L/b_{ij} + T_{propagation}$$

where:

- L is the size of the data packet (expressed in bits).
- $T_{propagation}$ is the propagation delay, which represents the time taken for the signal to travel from the starting place to the target (expressed in seconds).

The first term of the equation computes the time required to transmit the data packet over the network, determined by the bandwidth utilization *bij* and L denotes the size of the data packet. Propagation delay, indicating the time taken for the signal to propagate from the starting place to the target.
Proposed algorithm prioritizes selecting nodes with the highest available buffer and cache memory, smallest bandwidth usage. Additionally, it also considers the impact of mobility on system performance across various factors. Each node seeks out an efficient neighboring node to facilitate communication and reach the destination.

This approach ensures optimal resource utilization and efficient routing within the Vehicular Ad Hoc Networks environment. By selecting nodes with ample buffer and cache memory and minimal bandwidth usage, the algorithm aims to enhance data transmission reliability and minimize congestion. Moreover, considering mobility factors helps adapt routing decisions to dynamic network conditions, ensuring robust performance across varying scenarios. Overall, the algorithm promotes efficient and reliable communication while accounting for resource constraints and mobility dynamics within the VANET.

G. Proposed Algorithm

Algorithm-1: For selecting Most Reliable Path:

```
Step1:
   Read number of maximum nodes
Step2:
   Assign node ids to all vehicular nodes in the environment
Step3:
   Get node positions // Assuming all vehicle nodes have GPS
Step4:
   Set Cluster heads and Create clusters    // Cluster head selection based on algorithm 2
   clusterHeads = selectClusterHeads()    // Cluster formation based on Euclidean distance
   clusters = createClusters(clusterHeads)
Step5:
   After cluster formation, set routes     // Source node sends Route Request message (RRCP) to its
cluster head
   sendRRCPtoCH(sourceNode, CH1)
Step6:
   // Cluster head checks if the node is in its member list
   if nodeExistsInCluster(CH1.memberList, destinationNode):
      // Step 6a: If node exists in cluster, connect source to destination using intra-cluster routing
      intraClusterRouting(sourceNode, destinationNode)
```

```
    else:
        // Step 6b: Forward RRCP to Road Side Unit (RSU) or another Cluster head if node is not in the
cluster
        forwardRRCPtoRSU(RRCP, destinationNode)
Step7:
    // Further check the behavior of node for malicious nodes using algorithm 3
    checkForMaliciousNodes (sourceNode, destinationNode, reliablePath)
```

This pseudocode outlines the steps described in the algorithm. It includes functions for setting cluster heads, creating clusters, sending RRCP to the cluster head, checking if a node exists in a cluster, intra-cluster routing, forwarding RRCP to RSU, and checking for malicious nodes.

Algorithm for Route Discovery

```
Step1:
    // Source node sends Route Request message (RRCP) to its cluster head
    sendRRCPtoCH(sourceNode, CH)
Step2:
    // Cluster head checks the cluster member details for finding the destination
    if destinationNode in CH.memberList:
        // Step 2a: If destination exists in the cluster, establish route from source to destination directly
using intra-cluster routing
        intraClusterRouting(sourceNode, destinationNode)
    else:
        // Step 2b: Forward this request message to the Road Side Unit (RSU)
        forwardRRCPtoRSU(RRCP, RSU)
Step3:
    // Wait for the Route Reply message packet from destination
    waitForRREP()
Step3a:
    // If Route Reply (RREP) message received, start sending data packets
    startSendingDataPackets()
```

This pseudocode outlines the steps described in proposed algorithm. It includes functions for sending RRCP to the cluster head, checking if the destination exists in the cluster, intra-cluster routing, forwarding RRCP to RSU, waiting for RREP, and starting to send data packets upon receiving RREP.

Algorithm for Cluster member update

```
Step1:
    // If cluster member moves outside the range of the cluster head, update cluster member list
    if clusterMemberMovedOutsideRange(clusterHead, clusterMember):
        updateClusterMemberList(clusterHead, clusterMember)
Step2:
    // Cluster head estimates the current location of the cluster member
    estimateCurrentLocation(clusterHead, clusterMember)
Step3:
    // Cluster head updates its cluster member list
    updateClusterMemberList(clusterHead)
```

This pseudocode includes functions for checking if a cluster member has moved outside the range of the cluster head, estimating the current location of the cluster member, and updating the cluster member list.

Algorithm for Cluster head Re-selection

```
// Step 1: Periodically reselect the Cluster Head (CH) after a defined time interval
if timeElapsed(interval):
    reselectClusterHead()  // Function to trigger re-selection of CH
// Step 2: Ensure the CH is optimal based on its properties
if calculateMean(CH) < calculateMean(CM):  // Compare CH properties with average cluster member
properties
```

```
    // Step 3: Check if the cluster size is too small for effective clustering
    if clusterMemberCountInCluster() < 0.5 * CM:  // Ensure the number of cluster members is less than half of total CM
        // Step 4: Select a new CH based on geographic positioning
        selectMiddleClusterMemberAsCH()  // Choose a cluster member near the cluster center as the new CH
        // Step 4: This pseudocode includes functions for re-selecting the cluster head after a defined interval of time, checking if the mean of the cluster head's properties is less than the mean of the cluster members' properties, and selecting a cluster member in the middle of the cluster as the cluster head if the cluster size is less than half of the total cluster members.
```

Algorithm for Cluster merging

```
Step 1:
    // If distance between two clusters is less than initial distance, merge both clusters
    if calculateDistance(cluster1, cluster2) < initialDistance:
        mergeClusters(cluster1, cluster2)
Step 2:
    // If distance between CH1 and CH2 is less than 1/2 distance, form merged cluster CMx
    if calculateDistance(CH1, CH2) < 0.5 * distance:
        mergeClustersToFormCMx(CM1, CM2)
```

This pseudocode includes functions for calculating the distance between clusters and cluster heads, merging clusters, and forming a merged cluster CMx from CM1 and CM2.

Algorithm for Reliability Calculation

```
Step 1:
    // Save the copy of the original graph G
    originalGraph = copyGraph(G)
Step 2:
    // Declare a set S to save all paths from source to destination
    S = findAllPaths(S, G, S, D)
Step 3:
    // For all paths in set S, calculate shortest distance using Dijkstra's algorithm
    for each path in S:
        shortestDistance = Dijkstra(G, S, D)
Step 4:
    // Check the reliability of all paths using inclusion-exclusion algorithm
    for each path in S:        reliability = inclusionExclusiveAlgorithm(path, G, A)
```

This pseudocode includes functions for saving a copy of the original graph, finding all paths from source to destination, calculating the shortest distance using Dijkstra's algorithm, and checking the reliability of all paths using the inclusion-exclusion algorithm.

5. The Reliability Based Routing Protocol AODV-R

Expanding upon the well-established AODV routing protocol [26], we introduce our AODV-R routing protocol, with "R" denoting reliability. AODV-R enhances the reactive nature of AODV by establishing routes among starting place and target nodes only when necessary. This protocol is versatile, catering to both multicast and unicast routing scenarios.

Here's how AODV-R operates:

1. In a Vehicular environment when a network node requires a connection, it spreads a Routing Request Control Packet (RRCP) message to nearby Cluster Heads (CHs).
2. Upon receiving the RRCP, the CH search for the target node within its cluster member list.
3. If the target node is found, the CH forwards the RRCP to that node.
4. The target node responds to the starting place node with a Reply (RREP) message about the route, establishing the route.

This process ensures that routes are dynamically established between source and destination nodes, optimizing resource utilization and minimizing overhead. By integrating reliability considerations into

the AODV framework, AODV-R enhances the strength and efficiency of path fining in VANET environments.

1. The structure of the RRCP message is enhanced by introducing five additional fields:
   - XPos and YPos: These fields denote the vehicle coordinates responsible for generating or processing the RRCP.
   - Speed: Represents the vehicle velocity generating or processing the RRCP.
   - Movement angle: Indicates the vehicle direction generating or processing the RRCP.
   - Cluster Head ID: Identifies the cluster head associated with the vehicle node.
   - Route Reliability: This field signifies the consistency of the route.
2. Furthermore, an extra field is incorporated into the RRCP message structure:
   - Route Reliability Variable: This field embodies the ultimate value denoting the overall route consistency among the starting place and destination nodes. It assists the source node in selecting the most suitable route among various available options.
3. The routing table undergoes expansion through the inclusion of an additional field:
   - Route Reliability (route_reliability): This attribute stores the route consistency value corresponding to each route entry. Whenever a path with a greater consistency value for the similar target is discovered, relevant value is duly updated.

These expansions enhance the functionality and competence of the routing process in VANETs by providing additional information about vehicle coordinates velocity, direction, cluster head identification, and route reliability. This facilitates better route selection and management, leading to improved overall performance and consistency of the network.

6. Simulation Setup and Results

We simulated the proposed work and give subsequent performance assessments, using the MATLAB Simulator. The simulation setup involved emulating three lanes of traffic on a 5,000-meter highway, with vehicles travelling in two distinct directions. Each lane accommodated a constant presence of ten cars, and the data traffic flow was bidirectional, with vehicles looping back within the same path upon reaching the highway's end. This configuration facilitated ample opportunities for vehicle-to-vehicle communications and streamlined data delivery within the simulation.
Our simulation environment employed a highway mobility model, implemented within MATLAB and defined by Equations (4), (5), (6), (7), and (9), governing the movement patterns of vehicles within the simulated environment.

To simulate realistic traffic conditions, the average speeds of cars in each lane were set to forty, sixty, and eighty kilometers per hour, respectively. However, individual vehicle velocities varied to emulate the diverse driving behaviours observed on real roads.

In each simulation experiment, we set the R(P) that is known as reliability threshold to 0, signifying that the utmost consistency value determined the criteria selection at the end node. The subsequent simulation experiments were conducted as follows:

1. Experiment A: We progressively increased the regular speed of travel in the 3rd line from 60-140 km/h. Each UDP packet had a size of 1,024 bytes, and ten packets were transmitted per second.
2. Experiment B: We adjusted the size of data packet, ranging from 500–2500 bytes. It considers, ten packets were transmitted per second, with the average vehicle speeds set at 40, 60, and 80 km per hour for each lane, respectively.

These experiments were designed to measure the efficiency of the proposed AODV-R routing protocol under various traffic conditions, packet sizes, and transmission rates. By analyzing the simulation outcomes, we aimed to gain insights into the protocol's behavior across diverse scenarios and recognize possible areas for enhancement.

6.1. Performance Metrics

In our simulation experiments, we focus on evaluating the AODV-R routing protocol performance depending on the following four key performance metrics:

1. Packet Delivery Ratio (PDR): This metric indicates the number of successfully delivered data packets at the destination node in concern with the number of data packets sent by the source. A higher PDR value signifies more reliable and efficient data packet transmission within the network.
2. Link Failures: Link failures refer to the regular occurrences where communication links between nodes become unavailable during the path finding process. Monitoring link failures allows us to

gauge the robustness of the direction-finding protocol in maintaining continuous connectivity between network nodes.

3. Routing Control Overhead: This metric measures the ratio of all direction-finding control messages generated by the protocol to number of expected data messages received. It provides insights into the competence of the direction-finding protocol in managing routing-related overhead, such as route discovery and maintenance.
4. End-to-End Delay(E2E): It represents the standard time elapsed between the sending and receiving of data packets between the starting node and target node. Lower end-to-end delay values indicate faster and more efficient data delivery within the network.

By comprehensively evaluating these performance metrics in our simulation experiments, we aim to assess the performance of the AODV-R routing protocol under diverse network conditions and traffic scenarios. This analysis will help us understand the protocol's behavior and recognize any possible areas for development or optimization.

6.2. How Various Velocities Affect Routing Performance

As illustrated in Figure 2, the proposed AODV-R routing protocol surpasses AODV in terms of PDR. It's evident that with an boost in the average velocity in the 3rd row from 60-140 km/h, there's a decrease in the Packet delivery ration for both direction-finding protocols. This decline is attributed to the heightened instability and dynamism of the routing topology at higher velocities. However, AODV-R exhibits a slower decline in PDR compared to AODV. By prioritizing the selection of the most reliable path, AODV-R proves to be well-adapted to the dynamic road environment. When the starting node in AODV-R receives numerous direction-finding replies, it intelligently choose the most dependable path, thereby dropping the probability of connection failure and the necessitate for additional route discovery. This efficient path selection process conserves bandwidth, facilitating smoother data packet transmission with fewer interruptions.

In contrast, AODV demonstrates lower average end-to-end delay values compared to AODV-R, as depicted in Figure 3. This is because the route organization process in AODV-R involves processing numerous routing needs and replies, leading to longer delays. However, despite the delay, the recognized route in AODV-R remains reliable and stable over time. Also AODV prioritizes the shortest path to the end, regardless of its consistency.

Overall, while AODV-R may incur slightly higher E2E delay values due to its emphasis on reliability and stability, it ensures smoother and more dependable data transmission, particularly in highly dynamic road environments.

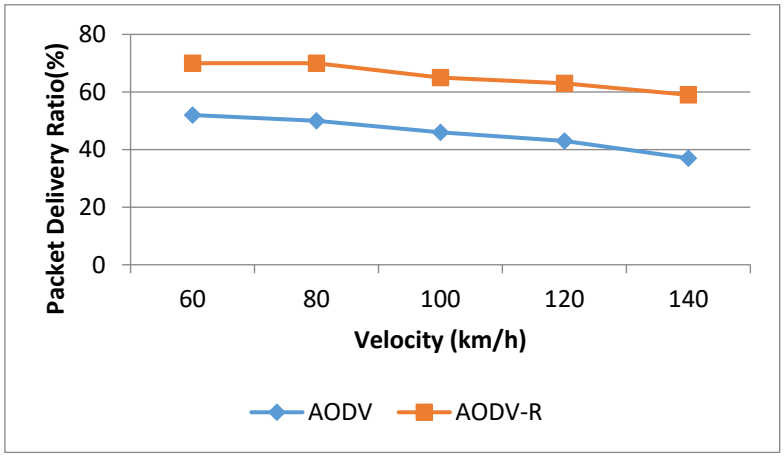

Figure 2. Average packet delivery ratio vs Velocity.

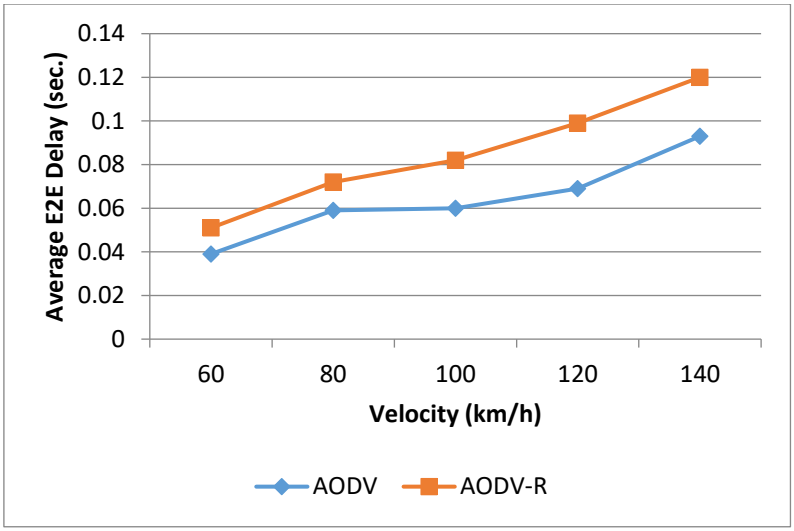

Figure 3. Average end-to-end delay v/s Velocity.

Indeed, within VANETs, the chances of link breakages increase due to the high movement of vehicles. However, the direct detection mechanism employed by AODV prioritizes speed, enabling it to identify routes more swiftly compared to AODV-R. This trade-off between speed and reliability becomes evident in Figure 3, where AODV demonstrates a lower average delivery ratio than AODV-R.

AODV's focus on expedited route discovery allows it to establish connections rapidly. But while achieving this efficiency we must compensate to the reliability, resulting in a decreased PDR, especially in scenarios with high velocities where link breakages occur more frequently. Conversely, AODV-R places a higher emphasis on reliability over speed, opting for more dependable paths even if the process of finding routes takes longer time. Consequently, AODV-R achieves a superior PDR, ensuring a greater number of data packet transmissions despite the challenges posed by the dynamic network environment.

In summary, while AODV may excel in quickly identifying routes, the reliability-centric approach of AODV-R proves advantageous in maintaining stable connections and achieving higher delivery ratios, particularly in environments characterized by high vehicle velocities where link breakages are prevalent.

Figure 4 depicts in case the link of data forwarding failure, the Route Error (RERR) message is triggered to resolve the issue by either repairing the currently found route or initiating a new process to find the route. As described in Figure 4, AODV encounters a greater number of failures compared to AODV-R. This disparity can be attributed to AODV's reliance on a shortest route selection algorithm, which renders it more susceptible to link breaks, especially in dynamic network topologies.

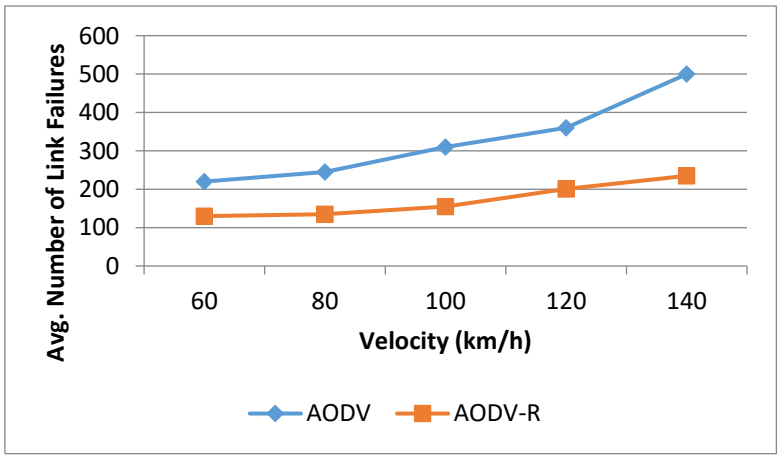

Figure 4. Average number of link failures v/s Velocity.

In contrast, AODV-R adopts a more comprehensive approach by evaluating all potential routes to the end node and prioritizing the dependable one. Consequently, AODV-R demonstrates a reduced speed of connection failures and exhibits greater adaptability to changes in the network topology, even amidst increasing velocities. AODV-R consistently maintains a lower rate of link failures compared to AODV.

This discrepancy underscores the efficacy of AODV-R's reliability-centric routing strategy, which

places emphasis on stable and dependable routes over speed. Through meticulous route evaluation and selection based on reliability metrics, AODV-R mitigates the impact of connection failures and ensures more resilient and robust communication in dynamic VANET environments.

Figure 5 showing the comparison among routing overhead among AODV and AODV-R. It showcases the effect of network architecture modifications on these routing protocols. Initially, it was anticipated that AODV-R would exhibit a greater routing manage overhead compared to AODV due to its utilization of higher manage messages for determining the most consistent route.

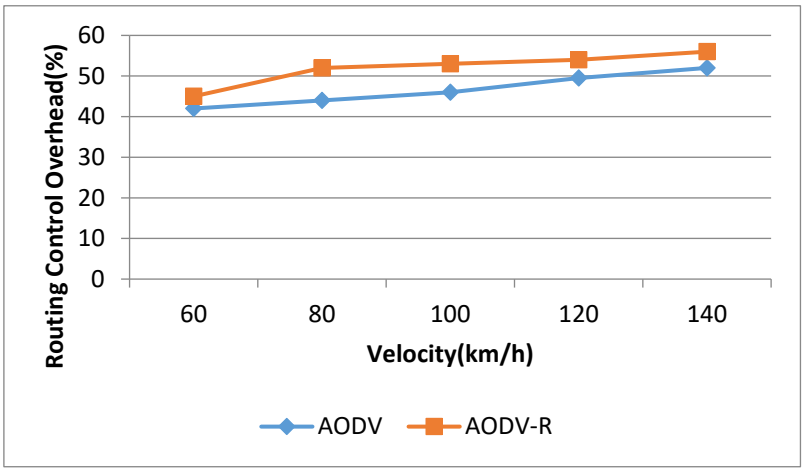

Figure 5. Average routing control overhead ratio v/s velocity.

Figure 4 further elucidates this point by illustrating how the higher link failures in AODV triggers the initiation of additional route discovery procedures, consequently leading to an increase overhead. Nonetheless, AODV-R demonstrates a more efficient management of direction-finding control messages, ensuring that the overhead remains comparable to AODV.

6.3. Routing Performance Related to Different Data Packet Sizes

As depicted in Figure 6 AODV-R consistently surpasses AODV in terms of PDR across various data packet sizes. However, it's worth noting that larger packets might be more prone to fragmentation, potentially introducing challenges in the packet delivery process. In cases where a connection failure occurs during the transmission of a data packet fragment, the entire data packet delivery process may fail, necessitating the initiation of a new route discovery procedure to establish an alternative route.

The introduction of additional route discovery processes leads to the generation of more routing control messages. Therefore, prioritizing the selection of the reliable path when delivering data packet fragments becomes crucial to mitigate the risk of encountering link failures.

In summary, while AODV-R demonstrates superior performance in terms of PDR compared to AODV, it's imperative to address potential fragmentation issues with larger packets and emphasize the selection of reliable paths to guarantee successful data packet delivery within VANET environments.

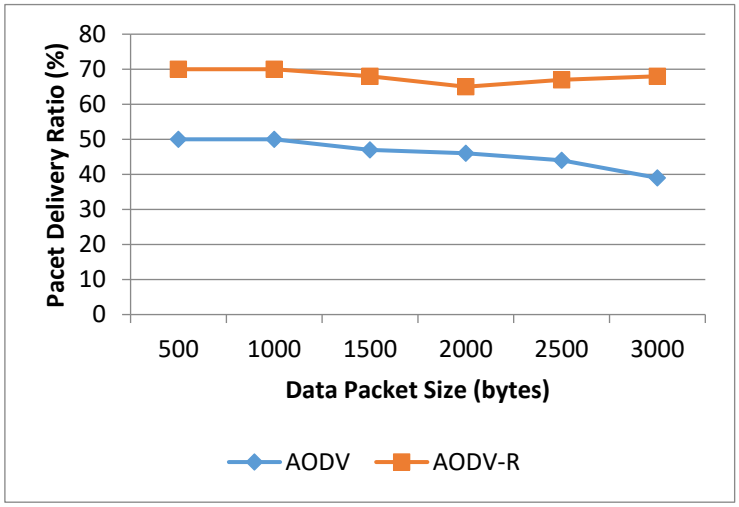

Figure 6. Average packet delivery ratio vs Data Packet Size.

Figure 7 of this experiment demonstrates that, in contrast to AODV, AODV-R also achieves a greater average E2E delay.

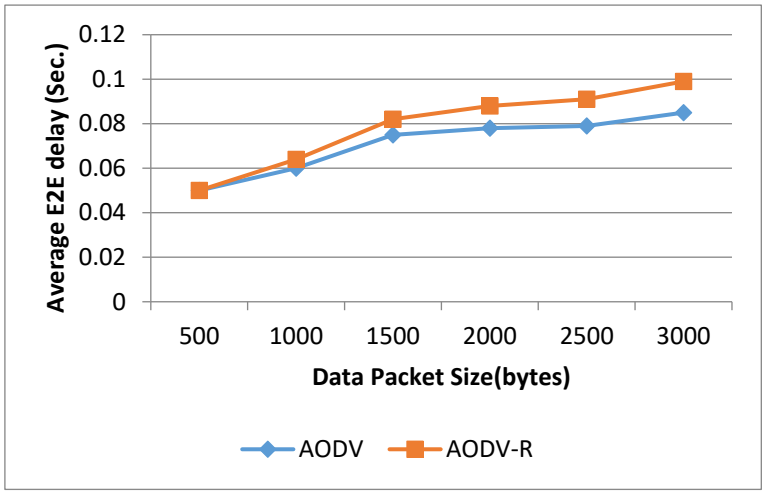

Figure 7. Average end-to-end delay vs Data Packet size.

Indeed, AODV-R's route establishment process may take longer compared to AODV, but the resulting route tends to be more reliable and stable over the period of time. AODV prioritizes the selection of the shortest path to the end node, leading to a quicker route discovery procedure. Figure 5 confirms this by showing that AODV exhibits a lower PDR than AODV-R.

Difference in PDR between AODV and AODV-R can be attributed to their respective routing strategies. While AODV focuses on speed and selects routes based on shortest paths, AODV-R prioritizes reliability and chooses the most dependable paths, even if it takes longer to establish them. Consequently, AODV-R achieves a higher PDR by ensuring more successful data packet transmissions, especially in dynamic VANET environments where link breakages are common.

Figure 8 confirms that AODV experiences a greater number of connection failures compared to AODV-R. This observation is further supported by Figure 5, which demonstrates that AODV-R achieves a high PDR than AODV. While the topology may not be highly dynamic, the simplistic path selection algorithm employed by AODV makes it more sensitive to link failures. In contrast, AODV-R actively seeks the Most Reliable Path(MRP), resulting in a lower rate of connection failures and improved overall network performance.

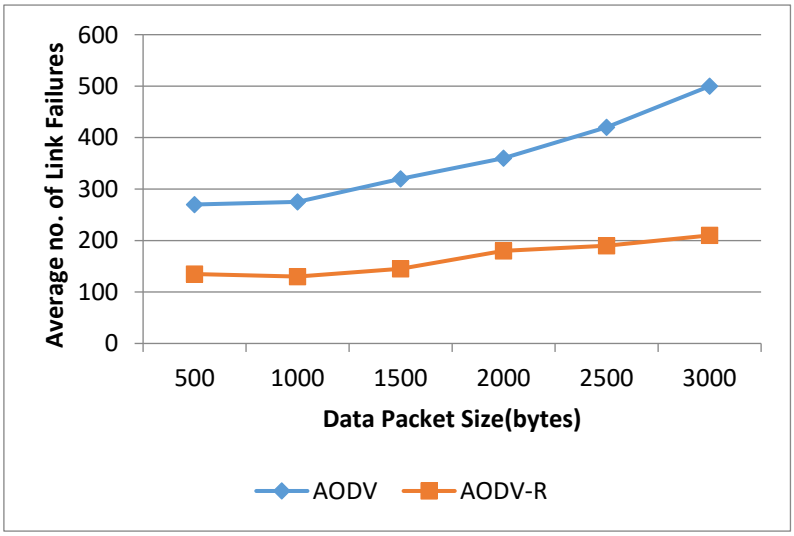

Figure 8. Average number of link failures v/s Data Packet Size.

Figure 9 depicted the average routing control overhead ratios. The elevated rate of connection failures

in AODV prompts more frequent route discovery processes, consequently contributing to heightened routing control overhead, as depicted in Figure 7. Nevertheless, AODV-R adeptly manages direction-finding control overhead by leveraging an increased number of direction-finding requests and responses to identify the MRP while ensuring that direction-finding control overhead remains within acceptable limits. Table 1 is depicting the Advantage of AODV-R over other State-of-Art algorithms.

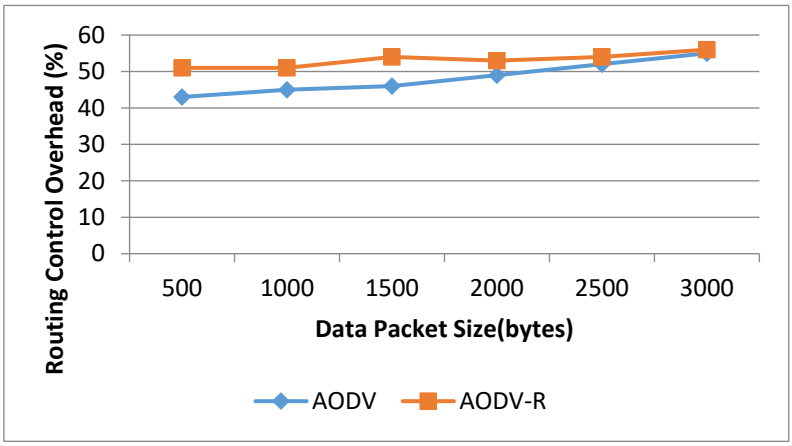

Figure 9. Average routing control overhead ratio v/s Data Packet Size.

Table 1. Advantages of AODV-R over other State of Art algorithms.

Feature	AODV [26]	AODV-R (Reliable AODV)	DSR [13]	OLSR [20]	GPSR [28]
Route Stability	Low	**High (Link stability prediction)**	Low	High	Moderate
Routing Overhead	High	**Reduced (Optimized RREQ, Clustering)**	High	High	Low
Security & Trust	Weak	**Strong (Trust-based Routing, Attack Mitigation)**	Weak	Moderate	Weak
QoS-Aware Routing	No	**Yes (Latency, Bandwidth, Link Quality Considered)**	No	No	No
End-to-End Delay	Moderate	**Low (Proactive Caching, Hybrid Routing)**	High	Low	Low
Load Balancing	No	**Yes (Traffic Distribution, Multi-path Routing)**	No	No	Moderate
Energy Efficiency	No	**Yes (Energy-Aware Routing for IoT-VANETs)**	No	No	Yes
Scalability	Moderate	**High (Cluster-based Routing, Optimized Broadcasts)**	Low	High	High
Mobility Adaptability	Moderate	**High (Mobility-Aware Metrics)**	Moderate	High	**Very High**
Loop-Free Routing	Yes	Yes	No	Yes	Yes

7. Conclusion

In this study, we introduced a novel connection reliability model it also taken into account the variability of vehicle speeds on highways, integrating it into the direction-finding process of VANETs to bolster reliability. Our proposed AODV-R direction-finding protocol, derived from AODV, incorporates this model and surpasses conventional AODV in terms of delivery ratio by prioritizing the selection of the most dependable path. Despite a slightly higher computational load, AODV-R experiences fewer link failures compared to AODV. However, it does exhibit somewhat high average end-to-end delays.

The connection reliability model identifies movement of the vehicles as the primary contributor to link breakages, with potential additional factors including congestion in the channel and noise errors. Future research extensions may explore the effect of these factors on the connection reliability model and how the path-finding protocol adapts to additional constraints like delay. In summary, this study lays the foundation for enhancing the reliability and performance of routing protocols in VANETs, providing valuable insights into mitigating link failures and enhancing data delivery in dynamic vehicular environments.

Future work can explore the scalability of the proposed algorithm in high-density networks, analyzing its impact on routing overhead, cluster stability, and QoS metrics like PDR and delay as vehicle density increases. Protocol's robustness can also been analysed by considering critical real-world factors like

urban obstructions, weather conditions, and varying vehicle speeds that can significantly impact VANET performance. Urban environments introduce signal attenuation and fading due to buildings and other obstacles, while weather conditions such as rain, fog, and snow can degrade signal strength and reduce communication range. So Nakagami fading model could use to simulate urban environments. Additionally, ITU-R P.838 attenuation models used for weather conditions. For vehicle speeds random mobility model cans been used.

Author Contributions
Conceptualization, Methodology, Paper writing and Validation: Mr. Wajid Ali.; Software usage support: Mr. Kamal Kumar Gola.; Review writing—Dr. Shalini Z. Nonoria, Supervision, Dr. Gulista Khan. All authors have read and agreed to the published version of the manuscript.

Funding
This research received no external funding.

Conflict of Interest Statement
Author declares no conflict of interest.

Data Availability Statement
Data is unavailable due to privacy or ethical restrictions, it will be provided on request to Correspondent author.

References

1. D. Jiang, V. Taliwal, A. Meier, W Holfelder, R. Herrtwich, Design of 5.9 GHz DSRC-based vehicular safety communication. *IEEE Wirel. Commun.* 13(5), 36–43 (2006)
2. W. Ali et. al. (2024), State of the Art, Reliable, and Trusted Communication in Vehicle to Everything (V2X) Networks, *Journal of Information Assurance and Security*, Volume 19 (2024): Issue 1 (August 2024). https://doi.org/10.2478/ias-2024-0001
3. H. Moustafa, Y. Zhang, *Vehicular Networks Techniques, Standards and Applications* (Auerbach Publications Boston, MA, USA, 2009), pp. 7–11. 111–115, 145–148
4. W. Ali et. al. (2024), Robust cryptographic scheme for reliable data communication in VANET (RCSRC) using clustering approach, EURASIP Journal on Wireless Communications and Networking, Alih et al. *J Wireless Com Network* (2024) 2024:82. https://doi.org/10.1186/s13638-024-02408-x
5. W. Ali et. al. (2024) Mechanism for Detecting and Preventing Security Attacks in VANET, In *Proceedings of the 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, https://doi.org/10.1109/IC3SE62002.2024.10593183
6. S. Jiang, D. He, J. Rao, A prediction-based link availability estimation for mobile ad hoc networks. *Proceedings of IEEE INFOCOM 2001*, Anchorage, AK 3, 1745–1752 (2001)
7. V. Thilagavathe, K Duraiswamy, Prediction based reliability estimation in MANETs with Weibull nodes. *Eur. J. Sci. Res.* 64(2), 325–329 (2011)
8. T. Taleb, M. Ochi, A Jamalipour, N Kato, Y Nemoto, An efficient vehicle-heading based routing protocol for VANET networks. *Paper presented at IEEE Wireless Communications and Networking Conference*, Las Vegas, NV, USA (3–6 April 2006)
9. K.T. Feng, C.H. Hsu, T.E. Lu, Velocity-assisted predictive mobility and location-aware routing protocols for mobile ad hoc networks. *IEEE Trans. Veh. Technol.* 57(1), 448–464 (2008)
10. A.A. Almazroi, M.A. Alqarni, M.A. Al-Shareeda, M.H. Alkinani, A.A. Almazroey, & T. Gaber, (2024). A Bilinear Pairing-Based Anonymous Authentication Scheme for 5G-Assisted Vehicular Fog Computing. *Arabian Journal for Science and Engineering*. 10.1007/s13369-024-09617-y.
11. Z.G. Al-Mekhlafi, S.A. Lashari, M.A. Al-Shareeda, B.A. Mohammed, A.M. Alayba, A.M. Saleh, S., K. Almekhlafi. (2024). CLA-FC5G: A Certificateless Authentication Scheme Using Fog Computing for 5G-Assisted Vehicular Networks. *IEEE Access*, pp. 1-1. 10.1109/ACCESS.2024.3466914.
12. A.A. Almazroi, M.H. Alkinani, M.A. Al-Shareeda, & S. Manickam. (2023). A Novel DDoS Mitigation Strategy in 5G-Based Vehicular Networks Using Chebyshev Polynomials. *Arabian Journal for Science and Engineering*. 49. 10.1007/s13369-023-08535-9.
13. Z.G. Al-Mekhlafi, S.A. Lashari, J. M. Altmemi, M.A. Al-Shareeda, B.A. Mohammed, A.A. Sallam, A.M. Alayba. (2024). Oblivious Transfer-Based Authentication and Privacy-Preserving Protocol for 5G-Enabled Vehicular Fog Computing. *IEEE Access*. pp. 1-1. 10.1109/ACCESS.2024.3429179.
14. V. Namboodiri, L. Gao, Prediction-based routing for vehicular ad hoc networks. *IEEE Trans. Veh. Technol.* 56(4), 2332–2345 (2007)
15. H. Menouar, M. Lenardi, F. Filali, A movement prediction-based routing protocol for vehicle-to-vehicle communications. *Paper Presented at the 1st International Vehicle-to-Vehicle Communications Workshop V2VCOM 2005, co-located with MobiQuitous 2005*, San Diego, California, USA (21 July 2005)
16. M. Nekovee, Sensor networks on the road: the promises and challenges of vehicular ad hoc networks and vehicular grids (*Paper Presented at the Workshop on Ubiquitous Computing and e-Research*, Edinburgh, UK, 2005)

17. D.B. Johnson, & D.A. Maltz, (2002). *Dynamic source routing in ad hoc wireless networks. In Mobile Computing* (pp. 153-181). Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-0105-0_5
18. K.C. Lee, U. Lee, M. Gerla, Survey of routing protocols of vehicular ad hoc networks, in *Advances in Vehicular Ad-hoc Networks: Developments and Challenges*, ed. by M Watfa (Information Science Reference, Hershey, PA, 2009), pp. 149–170
19. G. Yan, N. Mitton, X. Li, Reliable routing in vehicular ad hoc networks, In *Proceedings of the IEEE 30th international conference on distributed computing systems workshops (ICDCSW)*, Genova, Italy, 2010). 2125–263269
20. T. Clausen, P. Jacquet (2003). Optimized link state routing protocol (OLSR). In *Proceedings of the 2003 International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2003)*, 62-72. https://doi.org/10.1109/MOBIHOC.2003.1203983
21. M.H. Eiza, Q. Ni, A reliability-based routing scheme for vehicular ad hoc networks (VANETs) on highways. *Paper presented at the IEEE 11th international conference on trust, security, and privacy in computing and communications (TrustCom)*, Liverpool, UK , 1578–1585 (25–27 June 2012)
22. M. ul Hassan, A.A. Al-Awady, A. Ali, Sifatullah, M. Akram, M.M. Iqbal, J. Khan, Y.A. Abdelrahman Ali. ANN-Based Intelligent Secure Routing Protocol in Vehicular Ad Hoc Networks (VANETs) Using Enhanced AODV. *Sensors* 2024; 24(3):818. https://doi.org/10.3390/s24030818
23. D. Karunanidy, R. Rajakumar, A. Dumka, R. Singh, I. Alsukayti, D. Anand, & H. Hamam, M. Ibrahim, (2021). An Intelligent Optimized Route-Discovery Model for IoT-Based VANETs. *Processes* 9. 18. 10.3390/pr9122171.
24. S. Yousefi, E. Altman, R. El-Azouzi, M. Fathy, Connectivity in vehicular ad hoc networks in presence of wireless mobile base-stations. *Paper presented at the 7th Int. Conf. on ITS Telecommunication, Sophia Antipolis*, France (6–8 June 2007)
25. M.H. Eiza, Q. Ni, An evolving graph-based reliable routing scheme for VANETs. *IEEE Trans. Veh. Technol*. 62(4), 1493–1504 (2013). doi:10.1109/TVT.2013.2244625
26. S. Saeed, D. Mahtab, TGRV: A trust-based geographic routing protocol for VANETs, Ad Hoc Networks, Volume 140, 2023, 103062, ISSN 1570-8705, https://doi.org/10.1016/j.adhoc.2022.103062.
27. C.E. Perkins, E.M. Royer, Ad-hoc on-demand distance vector routing , In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99)*, New Orleans, Louisiana, USA, 1999), pp. 90–100
28. A. Silva, K. M. Niaz Reza and A. Oliveira, "An Adaptive GPSR Routing Protocol for VANETs," 2018 15th International Symposium on Wireless Communication Systems (ISWCS), Lisbon, Portugal, 2018, pp. 1-6, doi: 10.1109/ISWCS.2018.8491075.