Increasing Efficiency and Reliability in Multicast Routing based V2V Communication for Direction-Aware Cooperative Collision Avoidance

Original Scientific Paper

Lekshmi V.
Department of Computer Science and Engineering,
Noorul Islam, Centre for Higher Education,
Thackalay, Tamil Nadu, India
lekshmi123v@outlook.com

Suji Pramila. R
Department of Computer Science and Engineering,
Mar Baselios Institute of Technology and Science,
Kerala, India
sujipramila88r@gmail.com

Abstract *– Mobile ad hoc networks (MANETs), which are a promising method for the intelligent transportation system, include vehicular ad hoc networks (VANETs) (ITS). Developing reliable and strong cooperative collision avoidance (CCA) strategy to mitigate the growing number of road fatalities each year is one of the main difficulties facing vehicular ad hoc networks (VANETs).A proper and successful routing method aids in the successful expansion of vehicular ad hoc networks. This study explains the architecture, interface layers, safety features, and implementation of a novel priority-based direction-aware collision avoidance system (P-DVCA). It distinguishes our study in the collision area of VANETs by accounting for realistic bi-directional traffic. The scheme begins with the development of dynamic clusters, which is difficult because of the bi-directional diverse traffic and the need to avoid collisions within and between clusters. The target node is sent an early warning message that includes the safe speed and the likelihood of a collision in order to notify it of an impending danger. To determine the least expensive, shortest one with the fewest hops between the source and the endpoint. A crucial problem with VANETs is the transmission of data from a source node to the base station. Cross-layer issues must be solved for a robust and stable collision avoidance programme to function properly in a VANET communication architecture. The results of the simulation show that the suggested scheme significantly outperforms CCM and C-RACCA in terms of cluster stability, fewer collisions, low latency, and low communication overhead. According to the findings, P-DVCA offers stable clustering, minimises network congestion, and lowers communication overhead and latency.*

***Keywords**: Vehicular ad hoc networks, Intelligent transportation system, Collision avoidance, Direction-Aware Vehicular Collision Avoidance*

1. INTRODUCTION

The term "vehicular ad hoc network" (VANET) refers to a subclass of mobile ad hoc networks made up of mobile nodes made up of automobiles with wireless transceivers known as OBUs (On Board Units) that may collect, compute, receive, and broadcast data to other nodes [1]. In VANETs, each vehicle has the capacity to transmit data either directly to an external base station known as a Road Side Unit (RSU) through vehicle to infrastructure communication or between vehicles via vehicle-vehicle communication (V2V) (V2I) [2, 3]. It is necessary to deal with diverse information, such as traffic, roads, automobiles, and so on, in order to realise intelligent transportation [4]. Sharing information is crucial for preventing accidents, reducing traffic, and enhancing driving. In order to reduce traffic accidents, cooperative collision avoidance (CCA) methods assess impact rates between nodes on occasion and include the results in alert texts along with the appropriate preventive measures [5]. But in order to achieve effective collision avoidance in a CCA application, several issues need to be resolved at every level of the VANET communication architecture [6]. As a result, application layer collision probability computations are erroneous [7]. Furthermore, the performance of the current application layer protocols is negatively impacted by their reliance on preset decelerations as preventive measures [8]. Due to their large computational and communication overheads and unencrypted transmission of warning messages, the current security services layer architectures jeopardise message confidentiality [9]. Furthermore, it is discovered that the current VANET architectures are unable to handle the regular topological changes on bi-directional roads while routing warning messages [10]. One further significant drawback of the current VANET architectures is the unprioritized sending of warning messages at the MAC layer.

Problem Statement

It is found that existing VANET communication designs do not have a specific direction-aware communication architecture designed to reduce collisions on bi-directional roads. Furthermore, the collision prediction procedure is negatively impacted by the current architectures' failure to account for the direction component.

Contribution

The following contributions are made by the priority-based direction-aware collision avoidance (P-DVCA) protocol that we suggest:

- Priority-based direction-aware Collision avoidance, a novel CCA method (P-DVCA). The project uses a clustered environment and a V2V communication mechanism in a pure ad hoc architecture.
- As far as we are aware, P-DVCA is the first of its type to handle the more difficult and realistic highly dynamic heterogeneous bi-directional traffic scenarios in the collision avoidance domain of VANETs.
- Existing techniques, such as the collision computation model (CCM) in a unidirectional scenario and the cluster-based risk-aware CCA (C-RACCA). The existing technologies lack the ability to provide real-time bidirectional collision avoidance. However, we have proposed the priority-based direction-aware collision avoidance system (P-DVCA), which provides real-time bidirectional collision avoidance. The existing methods, CCM and C-RACCA, reduce the efficacy of CCA and delay in clock synchronization. The suggested P-DVCA results in a more dependable and efficient CCA by reducing network congestion when compared to the existing Methods.
- Results in quick clock synchronisation with a security service layer protocol protects the confidentiality of nodes, authenticates messages, and offers security for the delivery of secure alert notifications.
- A network layer protocol that, through greater channel utilisation, reduced communication overhead, and consideration of the orientations and relative positions of nodes, guarantees the timely and precise exchange of warning messages.
- The DCM suggested calculating the separation between the vehicles.

The remainder of the paper is structured as follows. Section 3 introduces the proposed method Experimental results and discussions are given in Section 4. Performance measures are in Section 5. Finally, conclusion and future work are presented in Section 6.

2. RELATED WORK

The performance and efficiency of VANET applications are major problems for transport systems these days, but these are usually related to the way messages are sent between the nodes. One of the primary issues is coming up with a better routing protocol for dynamic VANET systems [1].

Automobile clustering is a practical way to increase the network's scalability and connection stability. VANET features also impact the clustering's performance [2]. In addition to being impacted by the outside world, VANETs' communication efficiency is also more susceptible to malevolent attacks [3]. Message passing between neighboring base stations (BSs) and other multicast network functionalities are concentrated into the layer-2 of the BSs protocol stack in the proposed approach [4].

To determine the course from the Modified Zone Multicasting Routing Protocol (MZMRP) technique has been used in this study work to route data from the source node to the destination node. In this multicasting strategy, the network's root nodes are selected for data routing [11].

In order to achieve energy-efficient communication, a metaheuristic algorithm, such as the Enhanced Dragonfly Algorithm (EDA), which optimizes the parameter as minimum energy consumption in VANET, is used to identify efficient nodes from each cluster [5]. Future research can go in a number of different areas. Situations involving particular assaults (Sybil, Blackhole) on the hybrid trust model and look into how different groups communicate with one another and how different hops interact after the revocation process [6]. The CCAV-OLC strategy enabled the AVs to cooperate with one another, significantly reducing the danger of collision. The investigation of the network's capacity and communication range demonstrated the effectiveness of 6GV2X connectivity [12]. Based on contrasts of calculation cost and clash probable under various conditions, the proposed CCAV-OLC technique has an accuracy of 94.12% and reduces collisions by 87.23 percent [7].

Fuzzy logic has been used to enhance inter-vehicle geo cast routing. The suggested protocol used LET and PAD parameters as fuzzy system inputs to choose the most reliable link and prevent packets from being rebroadcast throughout the geographical region [9]. The overhead of the network, repeating packets, and link failure between two cars are reduced by using a dependable link [13].

The framework consists of three levels: the simulation of the VANET network is the first, followed by the reliability- and geometry-based routing criteria at the second level, and the routing algorithm at the third [14]. In VANET, a unique distributed tree generation distributed multicast routing technique was presented. The multicast route developed a dependable tree structure [15]. First, we create a vehicle mobility model at the crossings to forecast the connection time between vehicles. Then, in order to determine the physical layer transmission rate, we create a theoretical model of V2V communication [8]. The proposed method takes the nodes' mobility and bandwidth when creating an overlay tree [10].

The fuzzy-based cooperative MAC and prioritized message distribution protocol (FPMDC-MAC) is created [16]. It includes a priority assignment technique that takes into account the message type, severity level, and movement direction to improve the delivery of emergency warning signals. An Emergency Message Broadcast Protocol (EMBP) is suggesting [17]. By using a suboptimal relay node selection technique, we may ensure broadcast reliability while still choosing the best relay node based on factors like channel fading, mobility, and directionality [18].

Suggest a method for fusion location [19]. This method uses a hierarchical optimization strategy to incorporate light intensity measurements, inertial navigation data, and geomagnetic data [20]. Numerous routing protocols, such as unicast, multicast, broadcast, etc., have been proposed in the literature that takes advantage of the topology of the network.

3. PROPOSED METHOD

The delivery of warning signals must be prioritised under CCA schemes since they are time-sensitive. Giving warning messages a higher priority than non-warning communications is a promising strategy in this regard. This has a negative impact on the transmission of collision-prone warning messages, especially in congested networks.

3.1. PRIORITY-BASED DIRECTION-AWARE COLLISION AVOIDANCE (P-DVCA)

This section outlines our suggested P-DVCA protocol for transmitting V2V warning messages on dual lanes. The P-DVCA methodology begins with clustering the nodes in order to improve node manageability and to limit the broadcast areas. The node clock synchronisation that is necessary for time slot reservation comes next. Here, we present a method for synchronising local clocks that consists of two phases: synchronizations between and within clusters of clusters. P-DVCA structure is shown in Fig. 1.

P-DVCA is a protocol family with application, security, network, MAC, and physical layer components. Layer-by-layer characteristics of the suggested P-DVCA architecture. Using our variation of the dragonfly-based clustering technique, which was first presented in, application layer P-DVCA begins with nodes' clustering. The security services layer is in charge of securely transmitting warning signals in order to handle such urgent situations. Since nodes often enter and exit each other's communication range, frequent path rebuilding processes are required. Our three-tier priority assignment approach is used to send vital warning signals at a higher priority when MAC layer warning messages are time-sensitive.

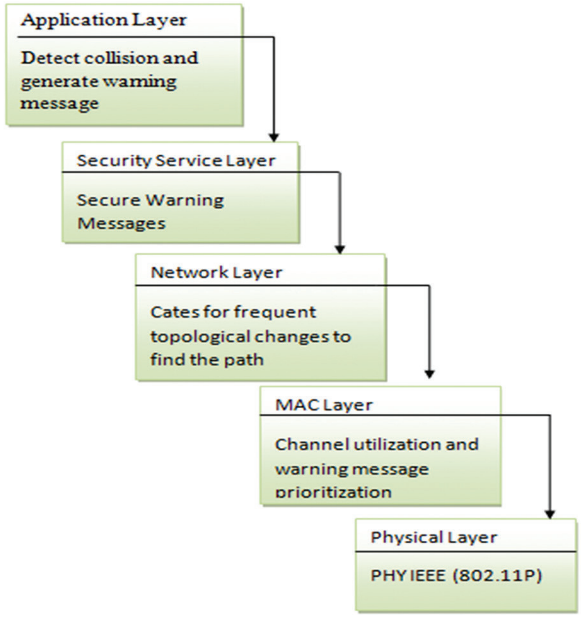

Fig. 1. P-DVCA structure

3.1.1. Application Layer

Our direction-aware CCA application is put into use by the P-DVCA application layer to specify preventive actions and identify potential collisions between nodes on bi-directional roads. The first metric, the Manhattan distance, determines the distance that exists between each neighbouring CH and an ideal node.

$$\eta = |X_1 - X_2| + |Y_1 - Y_2| \tag{1}$$

Where η Manhattan distance between the candidate node's coordinates (X_1-X_2) and (Y_1-Y_2), and the CHs is represented by the symbol. After calculating the Manhattan distance, the Hamming distance-which accounts for traffic flow in both directions is the second clustering metric.

$$k = \begin{cases} 1, & if\ \varphi = same \\ 0, & if\ \varphi = opposite \end{cases} \tag{2}$$

The importance of relying on the two indicators indicated above for node affiliation with clusters cannot be overstated. Assume that Node A is located 2 m from C2:CH and 3 m from C3: CH.

$$\delta = \frac{\eta}{K} \tag{3}$$

Where the separation (δ) between two neighbouring nodes is given. Eq. computes the distance to all surrounding CHs since P-DACCA only establishes an eligible node's link to a cluster when it is closest to the relevant CH. Where the separation (δ) between two neighbouring nodes is given. Eq. computes the distance to all surrounding CHs since P-DACCA only establishes an eligible node's link to a cluster when it is closest to the relevant CH.

3.1.2. Security service layer

When a malicious node intercepts a warning message meant to notify the target node to slow down in order to avoid a potential collision, it has the ability to either disregard the message or alter it in a way that will result in that collision. The security services layer is in charge of ensuring that warning signals are transmitted securely in order to overcome such dire circumstances.The security services layer is in charge of securely transmitting warning signals in order to handle such urgent situations. To do this, DVCA offers improved message authentication and node privacy preservation.

CH^i:

$$\beta_{CH^i} \leftarrow P_k \odot SID_{CH^i}$$

$$CH^i \ sends \ (\beta_{CH^i}||\tau) \ ton^i$$

n^i:

$$\beta_{n^i} \leftarrow P_k \odot SID_{n^i}$$

$$n^i \ sends \ (\beta_{n^i}||\tau) to \ CH^{\ i}$$

$CH^{\ i}$

$$CH^i \ generates \ key$$

$$key_i \leftarrow \beta_{n^i} \odot SID_{CH^i}$$

n^i:

$$n^i \ generates \ key$$

$$key_i \leftarrow \beta_{CH^i} \odot SID_{n^i}$$

Here, P_k stands for the public key, SID for a node's covert identity. The encrypted warning messages look like this.

Random generation of 1×4 matrix, Y

```
    For j=1 To 4
        Switch(Y(j))
Case 1:
            For x=1 To size(w) -1
            W(x)←w(x)⊕w(x+1)
            End For
            W←W⊕ Key_i
Case 2:
    W←Circular shift(W,C_s)
Case 3:
    Generate the random vector, rv
            w←w⊕rv
Case 4:
            Byte wise substitution operation
        End Switch
    End for
```

The warning message (W) that was obtained during the previously stated encryption process is then updated using the verification process hash that P-DVCA has generated.

$$\sigma_s = PID_s \odot PID_d \odot w \odot \tau \odot Key_i \tag{5}$$

In this case, PID stands for a node's public identification, which it uses to communicate with other nodes, and σ_s stands for the authentication hash created at the source node. To prevent blackhole attacks, a predetermined threshold is maintained that specifies how long warning messages should be retransmitted if the source nodes don't get any acknowledgements.

3.1.3. Network layer

Facilitating the prompt and dependable transmission of alert messages is the duty of the network layer. Due to high-speed nodes on bi-directional highways, VANETs frequently undergo topological modifications. Due to the frequent entry and exit of nodes inside each other's communication range, this causes frequent path rebuilding procedures. In addition to the distance parameter, P-DVCA adds two further parameters to account for these modifications. These parameters, which assist in determining the best appropriate path from the available set of paths, include the direction component and the relative positions of the source and destination nodes.VANETs frequently encounter topological changes. In order to deal with these changes, DVCA adds two more parameters in addition to the distance parameter. For a rear source node (S) with destination (D) having (S,) =1, the distance Δ between D and the subsequent hop (H) is calculated as

$$\Delta\ (D,H) = \frac{|H_x - D_x| + |H_y - D_y|}{k(S,H)} \tag{6}$$

In a case, where D remains rear to S, Δ is computed as

$$\Delta\ (D,H) = |H_x - D_x| + |H_y - D_y| k(S,H) \tag{7}$$

When S and D are travelling in opposing directions, D can be found using equation (6), and when they are travelling in the same direction, D can be found using formula (7). This type of direction-aware routing improves network performance. To ensure that warning messages are delivered on time, a direction-aware routing strategy optimizes network throughput by lowering packet drop rates and end-to-end delays. After that, the MAC layer receives the warning message from the network layer.

3.1.4. MAC Layer

P-DVCA synchronises clocks between and within clusters at the MAC layer. The effective completion of node clustering is followed by clock synchronisation. Nodes' familiar clocks are synchronised to a communal clock during the next two phases.

A. Syncing Clocks Across Clusters

The node's timer is regarded as synced and valid if $validate\_timer$ = 1. Conversely, if $validate\_timer$ = 0, no clock synchronisation is possible and the timer is still considered invalid by all other nodes in the network. Every node's admission to the highway requires clock synchronisation, which is why P-DVCA maintains the *validate_timer* default choice at 0.

The term "CH" refers to the collection of all CHs in the network that were chosen using the k-medoids algorithm. A CH is randomly selected from $\overline{CH}$ for this inter-cluster clock synchronisation, and is designated as "CH_B". The remaining CHs then follow the steps below to synchronise their local clocks with the CH_B shared clock. All reachable CHs respond to the clock synchronisation message (SyncCH) issued by CH_B.

B. Intra-Cluster Clock Synchronization

The method for synchronising clocks between and within clusters that has been proposed. Nodes can perform prioritised message dissemination after clock synchronisation; the process is described in more detail in the section below.

C. Prioritized Warning Message Dissemination

As illustrated in Table 1, there are three levels of warning messages: SL_0, SL_1, and SL_2. Here, SL_0 denotes the warning message with the lowest likelihood of collision, and SL_2 denotes the message with the highest likelihood of collision. When a warning message falls within the $SL0$ category, S waits for an $\urcorner_s$ available, maintaining this warning message type's lowest priority. By raising the priority level, SL_1 allows S to request the release of a space that was previously filled by $\urcorner_s$ warning message with a lower priority or a non-warning message. This guarantees the timely and accurate delivery of extremely important warning signals.

Table 1. Security level of warning message

Security level (SL)	SL Range	Limit of Probability of Impact (p_c)
SL_0	00	$0.00 < p_c \leq 0.33$
SL_1	01	$0.34 < p_c \leq 0.66$
SL_2	10	$0.67 < p_c \leq 1.00$
NW	11	$p_c = 0.00$

The algorithm requires the following inputs: S, D, R, $\propto_f$, -and W. R denotes the set of intermediary relay nodes$\propto_f$ denotes the set of free $\urcorner_s$, and W denotes a alert message. The algorithm's output consists of the choice of B_f and the reserve of s to transmit W.

Algorithm 1:
Prioritized warning message dissemination

Input: S, D, R, $\propto_f$, and W
Output: B_f selection and time slot reservation for warning message dissemination
Begin:
Repeat
If $D \in R$ Then
$S >> D$
Else
For i=1 **To** |size of(R)
$\mu_i \leftarrow |D_x - R_{i_x}| + |D_y - R_{iy}|$
$k_i \leftarrow H(R_i, D)$
If $H(S, D)$=1 Then
If S=Rear & D=Front node Then
$\delta_i \leftarrow \mu_i / k_i$
Else
$\delta_i \leftarrow \mu_i\, k_i$
End If
Else
IF S, D move towards each other **Then**
$\delta_i \leftarrow \mu_i / k_i$
Else
$\delta_i \leftarrow \mu_i\, k_i$
End If
End for
$B_f \leftarrow$Min(δ)
If $\propto_f = \emptyset$ Then
If W[SN_bit] = 1
$\ell \leftarrow W$[*severity-bits*]
Switch(ℓ)
Case:00
S waits for a free $\urcorner_s$
Case: 01
S requests to release a $\urcorner_s$
Case: 10
S releases $\urcorner_s$ already reserved by
A warning message that is not a warning or of lesser priority.
End Switch
Else
S waits for a free $\urcorner_s$
End If
Else
***S* reserver a** $\urcorner_s$ from$\propto_f$
End if
Until B_f=D
End

3.2. DISTANCE CALCULATION METHOD (DCM)

To calculate the distance between two vehicles, the DCM applies the distance formula. The DCM assumes that every car in the network has a GPS facility. The distance equation found in Eq.

Using Eq. 8, determine the distance D between A and B.

$$D_{ij} = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2} \quad (8)$$

The distance between two cars is represented by the D_{ij}. Equation 9 illustrates D_{ij}'s structure.

$$D_{ij} = D(i, j), edge(i, j) \in R \quad (9)$$

where D_{ij} is the measure of the separation between the cars. A route between cars is represented by R. The '*i*' and '*j*'stand for edges on route R. A route is a grouping of edges. Vehicle B uses Eq. 8 to determine the precise distance between two vehicles whenever it gets a beacon message from vehicle A. The distance computation method used to determine how far apart two cars are is shown in Fig. 2. In order to respond to the beacon messages, both vehicles operated in a promiscuous manner. The beacon is created and broadcast by First A. Upon receiving a beacon, every vehicle changes its corresponding routing table. The receiver vehicle routing tables contain computed D's.

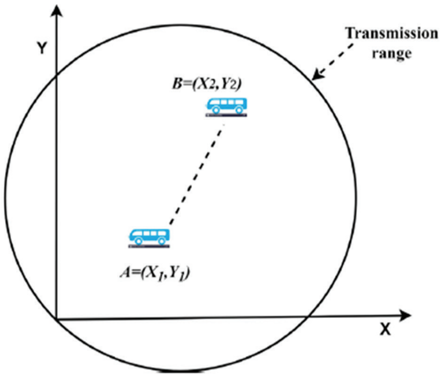

Fig. 2. Determining the separation between two cars

4. PERFORMANCE MEASURE

Comparing the performance of the suggested framework to the current plan allows for performance evaluation. The proposed approach is assessed in the simulator using the following performance metrics.

Packet Delivery Ratio (PDR):

This parameter shows the proportion between the total number of data packets generated during simulation and the total number of data packets received at the destination. The following Equation 3 can be used to calculate the Packet Delivery Ratio (PDR):

$$PDR = \frac{\sum_{ies} npacketReceived\ (i.d)}{\sum_{ies} npacketSent\ (i.s)} \quad (10)$$

Packet loss rate:

Calculated is the message loss rate (P_r).

$$P_r = \sum_{i=1}^{P_l} \frac{P_{l_i}}{P_t} \quad (11)$$

where P_{l_i} stands for a single message that is dropped and P_t stands for the total number of messages that were sent through the network. Choosing B_{fis} an important choice when transmitting warning messages.

End to End Delay:

The amount of time needed to transfer a packet from its source to its destination is known as the end-to-end delay (E2ED), and it may be calculated using Equation 10.

$$E2ED = 1/R \sum_{i=1...n} \sum_{j=1...ki} \left(r(Pij) - t(Pij)\right) \quad (12)$$

Throughput:

Routing protocols ought ideally to increase network performance since more data would be successfully routed via the network if they did.

$$\text{Throughput}=\frac{Number\ of\ received\ packets}{Total\ simulation\ time} * packet\ size \quad (13)$$

Routing overhead:

In order to make the message less stable for the recipient, extra bits are added to the packet containing the actual message at the MAC and physical layers. More data bits can be conveyed in a packet if the overhead is low since fewer bits are needed for information other than the actual data.

$$Overhead = \frac{totalPhybytes - totalAppBytes}{totalPhyBytes} \quad (14)$$

5. RESULT AND DISCUSSION

The simulation results are obtained using Python. Performance evaluation metrics include cluster stability, collision probability, packet destruction rate, packet delivery rate, complete delay, and throughput.

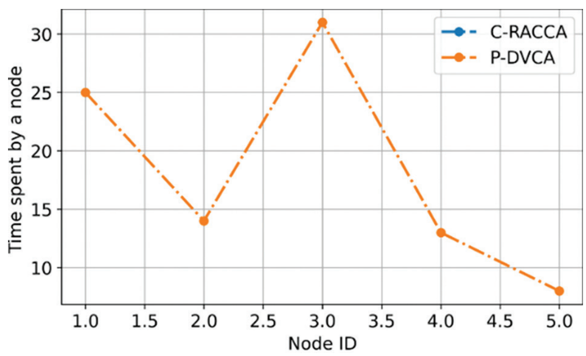

Fig. 3. Using C-RACCA and P-DVCA, node association to a cluster

Fig. 3. demonstrates the outcomes of P-DVCA and C-RACCA. Node 1 can be observed to spend the most of its time in C1. C-cluster RACCA's stability is hampered by this pointless cluster switch. In P-DACCA, the direction-aware clustering effectively corrects the aforementioned C-RACCA flaw. By maintaining constant relative speed, the effect of relative distance on collision is shown in Fig. 4.

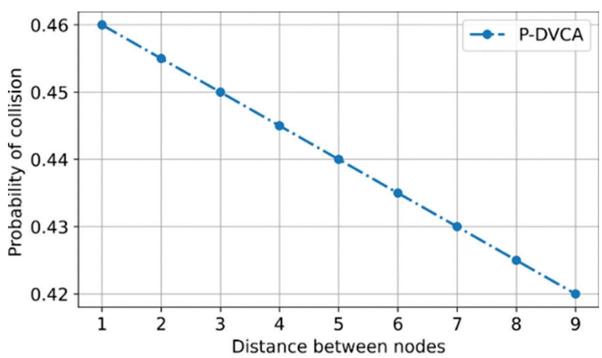

Fig. 4. By maintaining constant relative speed, the effect of relative distance on collision

Fig. 5 demonstrate a decrease in the likelihood of a collision as the distance between nodes grows, indicating that nodes are becoming safer at each stage.

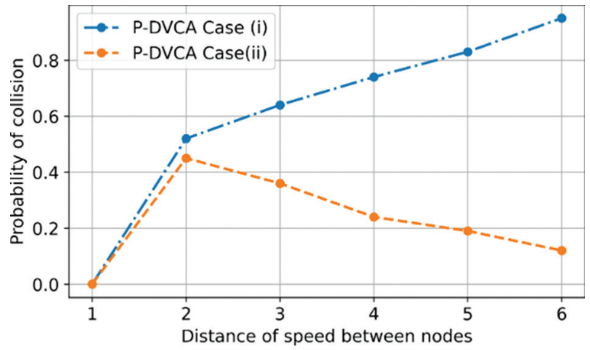

Fig. 5. Effect of relative speed on the likelihood of a collision given the expected state of the nodes and a constant relative distance

In scenario I the front node accelerates to a speed of 42 m/s and is followed by the rear node at a speed of 42 m/s. According to the results, the likelihood of a collision increases uniformly as the relative speed changes in relation to the front node's speed. This demonstrates the P-effectiveness DACCA's in estimating collision probabilities. When real-time nodes move along a highway, the distance also changes as the front node slows down. Although it is assumed that all of the individual occurrences occurring at various intervals are independent of one another, the relative distance is treated as constant in this simulation. Consequently, it shouldn't be mistaken for the front node's ongoing slowing. Similar to example I the rear node slows down by 4 m/s every time. The likelihood of a collision decreases when the rear node decelerates, in contrast to the front node. Each independent interval's estimated collision probability exhibits a linear decline. As a result, case (ii) also supports the usefulness of the suggested plan. Warning message generation is shown in Fig. 6.

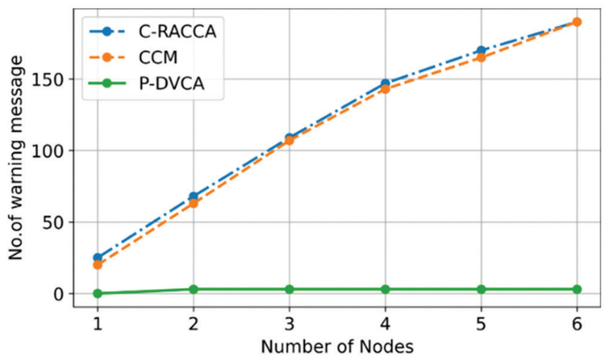

Fig. 6. warning message generation

P-DACCA, on the other hand, maintains the production rate constant regardless of the number of nodes. The extra communication overhead from these unnecessary warning messages contributes to network congestion, which reduces the effectiveness of CCA. P-DACCA creates a more reliable and efficient CCA by reducing network congestion.

In Fig. 7. it is quite clear that P-DVCA doesn't provide any pointless warning messages. For C-RACCA and CCM, on the other hand, the generation rate of pointless warning messages continues to be very high and grows exponentially as the number of nodes rises.

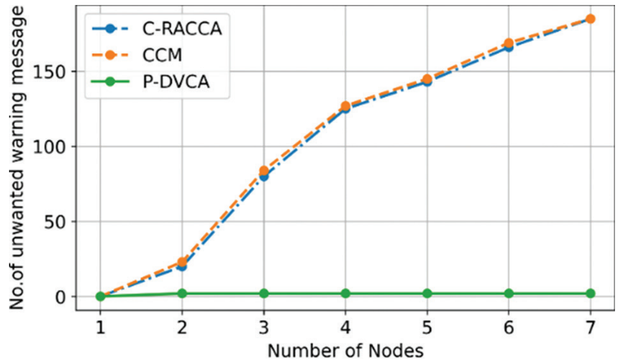

Fig. 7. creation of unwanted warning messages

The findings in Fig. 8 demonstrate the impact of an increase in hop count on warning message transmission latency. Due to the reduction in reaction time to implement preventative actions caused by the warning message transmission delay, the likelihood of accident increases.

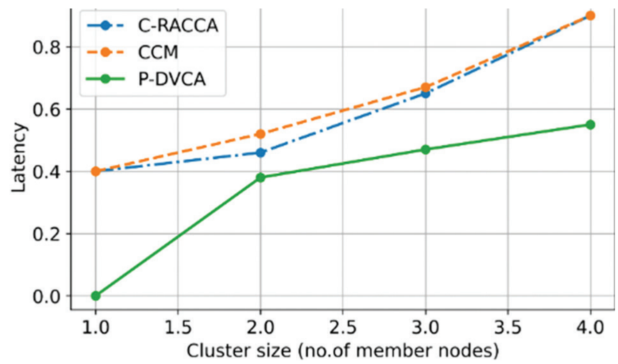

Fig. 8. Effect of hop count on warning message transmission latency

The number of $\daleth_s$ on the frame continues to be inversely correlated with the quantity of messages. As a result, each $\daleth_s$'s duration also changes or lengthens in accordance. This suggests that a higher network traffic load reduces the frame's $\daleth_s$ duration in P-DVCA, which increases end-to-end delay. Due to these factors, P-DVCA performs better than C-RACCA and CCM, as evidenced by the findings in Fig. 9 a. The findings in support the higher throughput achieved by P-DVCA when compared to C-RACCA and CCM thanks to our ground-breaking three-tier priority assignment method. In the outcomes reported in Fig. 9 b, P-DVCA also maintained its superiority over C-RACCA and CCM. When a relay node faces away from the destination node, the likelihood of a network partition rises, which ultimately leads to a higher rate of message loss. The findings shown in Fig. 9 c support this assertion. Fig. 9 d's findings reveal that P-DVCA has the least amount of communication overhead when compared to C-RACCA and CCM.

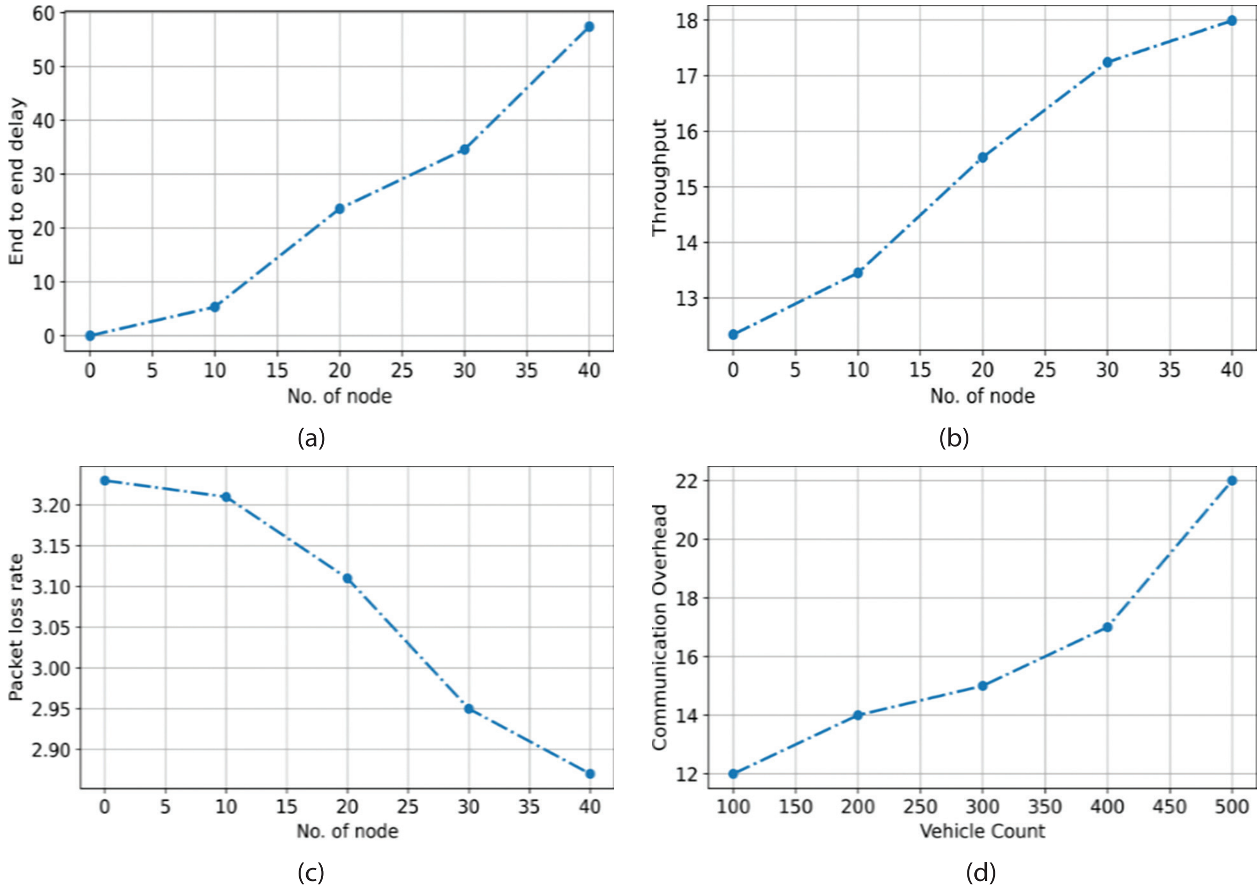

Fig. 9. Performance parameter of (a) End-to-End Delay, (b)Throughput, (c) Packet loss rate, (d) Communication overhead

6. CONCLUSION

P-DVCA offers a CCA scheme for bi-directional highways in an effort to close this gap. In an effort to provide a safe driving environment, it offers an effective method for reducing traffic accidents. P-DVCA is a clustered V2V technique that handles both intra- and inter-cluster collision avoidance utilising a pure ad hoc VANET architecture. To the best of our knowledge, bi-directional traffic has never before been present in the crash-avoidance region of the VANET. In order to guarantee the prompt and accurate delivery of alert texts, top billing allocation in P-DVCA in the message type, severity level, and direction component of nodes. the formation of steady clumps. After clustering, the nodes' anticipated states are calculated. Some projected states are used to determine the probability of a collision between every pair of connected units. In addition to threshold-based message distribution, the communication overhead is decreased by avoiding unnecessary warning messages. The findings demonstrate that P-DVCA offers reliable clustering, little network slack, decreased latency, and reduced communication overhead.

7. REFERENCES:

[1] E. Khoza, C. Tu, P. A. Owolawi, "An Ant Colony Hybrid Routing Protocol for VANET", Proceedings of the International Conference on Intelligent and Innovative Computing Applications, Mon Tresor, Mauritius, 6-7 December 2018, pp. 1-6.

[2] M. K. Jabbar, H. Trabelsi, "Clustering Review in Vehicular Ad hoc Networks: Algorithms, Comparisons", Challenges and Solutions. International Journal of Interactive Mobile Technologies, Vol. 16, No. 10, 2022.

[3] H. Xia, Z. San-shun, L. Ben-Xia, L. Li, C. Xiang-Guo, "Towards a Novel Trust-Based Multicast Routing for VANETs", Security and Communication Networks, Vol. 2018, 2018.

[4] S. Roger, D. Martín-Sacristán, D. Garcia-Roger, J. F. Monserrat, P. Spapis, A. Kousaridas, A. Kaloxylos, "Low-latency layer-2-based multicast scheme for localized V2X communications", IEEE Transactions on Intelligent Transportation Systems, Vol. 20, No. 8, 2018, pp. 2962-2975.

[5] M. Elhoseny, K. Shankar, "Energy efficient optimal routing for communication in VANETs via clustering model", Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks, Vol. 242, Springer, 2020, pp. 1-14.

[6] H. Hasrouny, A. E. Samhat, C. Bassil, A. Laouiti, “A security solution for V2V communication within VANETs”, Proceedings of Wireless Days, Dubai, United Arab Emirates, 3-5 April 2018, pp. 181-183.

[7] A. Malathi, N. Sreenath, “Multicast routing selection for VANET using hybrid scatter search ABC algorithm”, Proceedings of the IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, Chennai, India, 21-22 September 2017, pp. 441-446.

[8] X. Fan, Y. Lu, B. Liu, D. Liu, S. Wen, B. Fu, “High-integrity based cooperative file transmission at urban intersections using pure V2V communication”, Ad Hoc Networks, Vol. 122, 2021, p. 102612.

[9] A. Malathi, N. Sreenath, “Improved Shuffled Frog-Leaping Algorithm Based QoS Constrained Multicast Routing for Vanets”, Wireless Personal Communications, Vol. 103, 2018, pp. 2891-2907.

[10] P. K. Swetha, “An Improved Cluster based Multicasting Technique on Vehicular Adhoc Network”, Proceedings of the Second International Conference on Green Computing and Internet of Things, Bangalore, India, 16-18 August 2018, pp. 263-267.

[11] S. Ali, A. Chaudhary, H. Pasricha, “A novel modified zone multicasting routing protocol for path establishment in VANET”, International Journal of Computer Science and Network, Vol. 9, 2020, pp. 38-45.

[12] S. B. Prathiba, G. Raja, N. Kumar, “Intelligent cooperative collision avoidance at overtaking and lane changing maneuver in 6G-V2X communications”, IEEE Transactions on Vehicular Technology, Vol. 71, No. 1, 2021, pp. 112-122.

[13] E. Moridi, H. Barati, “Increasing efficiency and reliability in multicasting geographical routing based on Fuzzy Logic in VANETs”, Journal of Soft Computing and Information Technology, Vol. 12, No. 39, 2020, pp. 11-19.

[14] S. A. Rashid, M. Alhartomi, L. Audah, M. M. Hamdi, “Reliability-Aware Multi-Objective Optimization-Based Routing Protocol for VANETs Using Enhanced Gaussian Mutation Harmony Searching”, IEEE Access, Vol. 10, 2022, pp. 26613-26627.

[15] S. Babu, A. R. K. Parthiban, “DTMR: An adaptive distributed tree-based multicast routing protocol for vehicular networks”, Computer Standards & Interfaces, Vol. 79, 2022, p. 103551.

[16] M. Manoj, A. Ch Sudhir, “Fuzzy Based Prioritized Message Dissemination and Cooperative MAC Protocol for VANET", Wireless Personal Communications, Vol. 133, 2023, pp. 1175-1198.

[17] Z. Xiang, Y. Zhang, Y. Chen, Y. Ma, H. Cao, L. Tian, "Emergency message broadcasting scheme based on V2V and V2I", ITU Journal on Future and Evolving Technologies, Vol. 4, No. 4, 2023, pp. 549-561.

[18] M. Bilal, E. U. Munir, A. Ullah, "BEMD: Beacon-oriented Emergency Message Dissemination scheme for highways", Ad Hoc Networks, Vol. 142, 2023, p. 103095.

[19] Y. Han, X. Yu, P. Zhu, X. Xiao, M. Wei, S. Xie, "A Fusion Positioning Method for Indoor Geomagnetic/Light Intensity/Pedestrian Dead Reckoning Based on Dual-Layer Tent–Atom Search Optimization–Back Propagation", Sensors, Vol. 23, No. 18, 2023, p. 7929.

[20] M. Sohail, Z. Latif, S. Javed, S. Biswas, S. Ajmal, U. Iqbal, M. Raza, "Routing protocols in Vehicular Adhoc Networks (VANETs): A comprehensive survey", Internet of Things, Vol. 23, 2023, p. 100837.