Implementation of a Secure and Efficient Routing Algorithm for Vehicular Ad Hoc Networks

M. N. Prashanth(✉) and Annapurna P. Patil

Ramaiah Institute of Technology, Bangalore 560054, Karnataka, India
mnprashu@gmail.com, annapurnap2@msrit.edu

1 Introduction

1.1 Vehicular Ad Hoc Networks

Vehicular ad hoc network is a form of ad hoc network wherein intelligent vehicles take part in communication. Ad hoc network does not rely on infrastructure for communication with this principle; VANETs have additional constraint, highly dynamic environment.

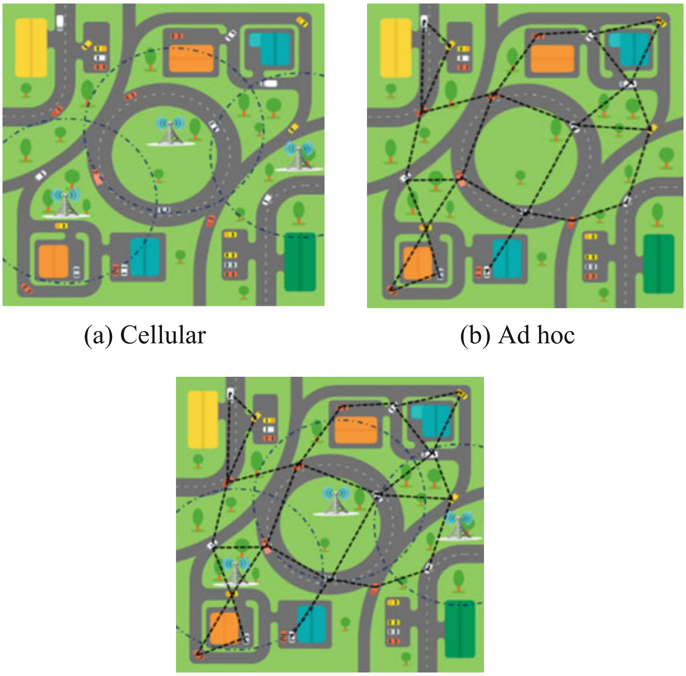
The architecture of VANETs falls under three categories cellular, ad hoc, and hybrid. As shown in the Fig. 1a, the access points are used for communication among the vehicles. These access points are installed at traffic intersections. Access points have their own advantages and limitations, and they have a fixed range for communication; moreover, the fixed infrastructure incurs more cost and also the maintenance cost. Best way to overcome is to have ad hoc network as shown in Fig. 1b; the vehicles form a network and communicate among themselves. Finally, the third kind is combination of both cellular and ad hoc shown in Fig. 1c; this incorporates the features of both cellular and ad hoc architecture. Namboodiri et al. [1] proposed such a hybrid architecture, which uses some vehicles with both WLAN and cellular.

1.2 Basic Characteristics

Vehicular ad hoc networks comprise vehicles which act as mobile nodes and also routers for other vehicles. VANETs have unique characteristics in addition to ad hoc networks characteristics such as dedicated short-range communication, self-organizing, and configuring, which distinguish it from other ad hoc network. The basic characteristics are as follows [2]:

1. Highly dynamic environment: The topology of VANETs changes frequently due to high-speed movement between vehicles. For example, the link among vehicles exists if they fall under the transmission range. In case of vehicle moving in opposite direction with high speed, the link lasts only few seconds; this makes the topology to break.
2. Frequent link failure: Due to high dynamic topology, the connection among the vehicles get disconnected frequently. Especially in the low density, the probability of link failure is higher.

S. Bhattacharyya et al. (eds.), *Advanced Computational and Communication Paradigms*, Lecture Notes in Electrical Engineering 475,
https://doi.org/10.1007/978-981-10-8240-5_27



(a) Cellular (b) Ad hoc

(c) Hybrid

Fig. 1. Vehicular ad hoc network architecture

3. Communication environment: Typically, VANETs' communication falls under two scenarios: highway traffic and street in a city, where the communication is complex and no direct communication as it comprises more obstacles (buildings, trees). In the latter case, it is simple and straightforward as it has one-dimensional movement.
4. Sufficient energy and processing: VANETs have sufficient processing power and energy compared to the small mobile handheld devices.
5. Geographical type of communication: To forward packets in geographical area, VANETs have a new type of communication unlike other networks where multicast and unicast are used.
6. Delay constraints: For safety applications, the messages should be communicated within certain time. In this case, the network need not to have high throughput but the constraint is on delay. Network should have minimum delay.

2 Related Work

In [3], author considers the vehicles which are few hops away in the network for the routing. Considering the small-scale network with few hops, the traditional algorithm AODV is applied. However, the routes determined by the algorithm prone to frequent breaks due to dynamic mobility. The author proposed prediction-based algorithms which are PRAODV and PRAODVM; both the algorithms use acceleration and position of the vehicles to predict the path lifetime. The simulation results of the proposed work showed considerable improvement with respect to packet delivery ratio (PDR). The algorithm performance highly depends on the outcome of prediction accuracy.

In [4] AODV protocols has been altered to forward the request within the zone, i.e., zone of relevance (ZOR). ZOR has a fixed range for the communication. The range is determined by the nature of the application [5]. The idea is similar to that of location aided routing [6].

In [7], the author proposed a location-based algorithm called LORA_CBF, which uses flooding concept. In this, each node can be a gateway, cluster head, or member. Similar to the greedy algorithm, the packets are forward. If the destination location is not known, the source node initiates the location request (LREQ) packet. This is similar to that of AODV route discovery phase, but in this case, the dissemination of the packet, i.e., LREQ and LREP, is done by the cluster heads and gateway only. The simulation results showed that performance of AODV and DSR was significantly lower than LORA_CBF due to the constraint scalability and mobility.

3 Proposed Algorithm

In VANETs, because of highly dynamic topology, discovering and maintaining route is a challenging task. Many routing protocols were proposed, which are classified under the following category ad hoc, position based, broadcast, geocast, and cluster-based routing. As stated earlier, the VANETs incorporate the features of ad hoc network. The routing protocols like AODV [8] and DSR [9] are still applicable for VANETs, but they are designed for general ad hoc network; the route maintenance is not done unless it is required. However, in case of VANETs, due to dynamic topology, it is unable to find the route quickly and also, it is difficult to update and maintain the route information. This degrades the performance as packets are lost due to frequent route failure. Therefore, the routing protocol must possess the following features: (1) better route convergence time and (2) rate of link failure should be minimal.

The bio-inspired routing protocol AntHocNet [10] uses ant agents to discover and maintain the route. The algorithm has proven its performance with respect to route convergence time and rate of link failure for mobile ad hoc networks (MANETs). But for VANETs, the direction and speed of moving vehicle need to be considered. In this paper, we describe how the AntHocNet algorithm is modified to improve the performance considering the direction of the moving vehicle.

In the proposed algorithm, two cases are considered during routing phase: (1) destination vehicles moving in the same direction as of source and (2) destination vehicle moving in opposite direction. Figure 2a, b shows the proposed algorithm for destination vehicle moving in the same and opposite direction to that of source. In the proposed algorithm, the forward ants are generated at the intermediate nodes only if the criterion is satisfied. In case of destination moving in the same direction as of source, the axis of moving nodes is compared with that of source; if it matches, then that node will take part in the routing as an intermediate node. The process continues until the destination is reached. In case of destination vehicle moving opposite to source, nodes moving in the direction of destination are considered to take part in the routing process as an intermediate node.

```
Algorithm: Nodes moving in same direction
Begin:
        Generate the ants to find the route between the pair of nodes.
        If node is destination
        Begin:
                Generate the backward ants
                Halt
        End
        Else if it is an intermediate node
        Begin:
                If the node is moving in the same lane
                Begin:
                    Generate the forward ants
                End
                Else
                Begin:
                    Discard
                End
        End
End
```

```
Algorithm: Nodes moving in opposite direction
Begin:
        Generate the ants to find the route between the pair of nodes.
        If node is destination
        Begin:
                Generate the backward ants
                Halt
        End
        Else if it is an intermediate node
        Begin:
                If the node is moving in the opposite lane
                Begin:
                    Generate the forward ants
                End
                Else
                Begin:
                    Discard
                End
        End
End
```

Fig. 2. **a** Destination node moving in the same direction as of source, and **b** destination node moving in opposite direction to that of source

The networks are prone to attack, which often leads to poor performance. There are different types of attacks; few of them are attacks on identification and authentication, attacks on privacy, attacks on availability, network denial of service (DoS), and attacks on data trust. In this paper, the attack on availability of the resource is described. In the hybrid architecture of VANETs, the roadside units (RSUs) act as a communication end point. The vehicles use the RSUs to transfer messages to other vehicles. In a safety application and smart transport system, RSUs act as a focal point wherein the crucial and traffic-related information are disseminated from RSUs. Therefore, RSUs act as a crucial resource which needs to be secured from attack. As stated earlier, the attack on availability is addressed. RSUs have the capability to process the requests that are sent from different vehicles and meantime, it also performs its own computation.

In VANETs, vehicles have sufficient energy and processing capability. But RSUs are devices that are installed at the road junction points to disseminate the messages during the critical situation; therefore, we assume that it has minimal energy and processing capacity. RSUs may get detached from the network due to low energy during the DOS attack, as it consumes more energy to process junk requests that are generated from the malicious nodes, which impact on the availability of RSUs.

In the proposed algorithm (Fig. 3), the minimum and maximum threshold values for energy are defined. The algorithm periodically monitors the network; if the nodes energy fall below the minimum threshold value, then that node is treated as victim of DOS attack. The algorithm identifies the malicious nodes by considering the maximum threshold values of energy and deactivates those nodes from the network. The pseudocode of the algorithm is shown in Fig. 3.

```
Algorithm: Identifying the malicious node
Begin:
        Periodically monitor the network nodes
        Check for nodes energy level
        If energy of the node is below the min threshold value
        Begin:
                Identify the nodes that has energy level more than the max threshold
                value
                  If found
                  Begin:
                          Deactivate the node
                  End
        End
End
```

Fig. 3. Identifying the malicious node

4 Simulation Environment

Table 1 summarizes the QualNet configuration setup under which the proposed algorithm is simulated and evaluated its performance with respect to the existing protocols.

The simulation is executed for 660 s, during which vehicles were configured to move in a fixed mobility path using fixed waypoint mobility model. The density of the vehicles is increased in the interval of 20 nodes (20, 40…). The granularity of the movement has been varied from the range 0.1–1.0 m. The simulation has been set up for the 2500 × 2500 urban terrain; totally, 12 RSUs were set up for the better

Table 1. Simulation configuration setup

Simulation tool	QualNet 7.4
Terrain (dimension)	2500 × 2500
Number of nodes (vehicles)	20, 40, 60, 80
Number of RSUs	12
Granularity (in meters)	0.1, 0.5, 1.0
MAC protocol	MAC 802.11p
Routing protocol	AntHocNet, Proposed_AntHocNet, AODV
Simulation time	660 s

communication at the road junction points. All the vehicles and the RSUs were configured to use MAC 802.11p protocol.

4.1 Simulation Results

The proposed algorithm has been compared with the existing algorithm with respect to varies performance metric, viz., throughput, average end-to-end delay, average jitter, network lifetime, average energy consumption, and number of link failures, after running extensive test cases. The primary focus of the proposed algorithm is to reduce the frequent link failure and to defend the network during the attack on availability. The performance of the proposed algorithm with respect to link failure and the energy consumption with attack and without attack are described in this section.

Frequent Link Failure

VANETs are highly dynamic in nature; the topology of the network changes frequently due to its high mobility; because of this, the communication link breaks frequently which degrades the performance of the network.

Figure 4 shows the number of link failures under the environment of 20 nodes with the varying granularity. It is observed that with low granularity the proposed and existing AntHocNet algorithm has no change in the link breaks as the granularity has been increased the proposed algorithm has better performance compared to existing algorithm. Both the existing and proposed algorithms have better performance compared to traditional AODV algorithm.

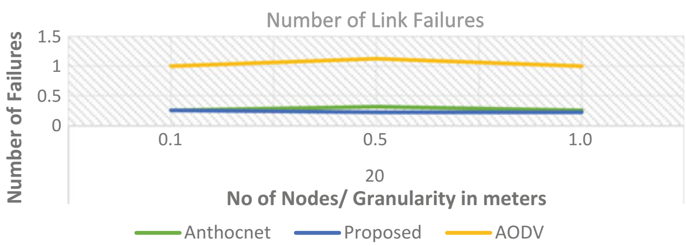


Fig. 4. Number of link failures under 20 nodes and varying granularity

Figure 5 shows the overall performance of the network with respect to number of link failures under the sparse, moderate and dense environment. From the figure, it is inferred that, when the granularity and also the number of nodes participating in the network are low, the number of link failures is less. As the granularity increases, the number of link failures also increased in the proposed algorithm but considerably less compared to the existing AntHocNet. In case of high granularity and moderate environment, the proposed algorithm has less number of link failures compared to the existing algorithm.

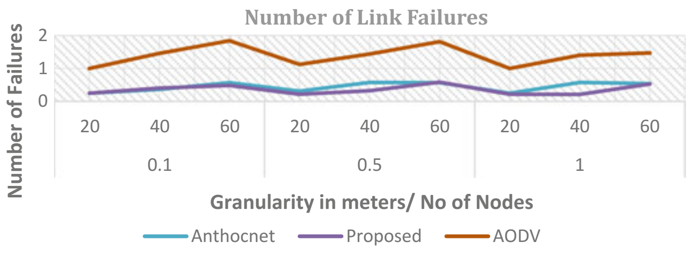


Fig. 5. Number of link failures under 20, 40, 60 nodes and varying granularity

From Fig. 6, it is observed that the enhanced algorithm has less delay compared to the traditional AntHocNet. It is also observed that there is no significant change in delay for both the enhanced and traditional AntHocNet over the network consisting of 40 nodes.

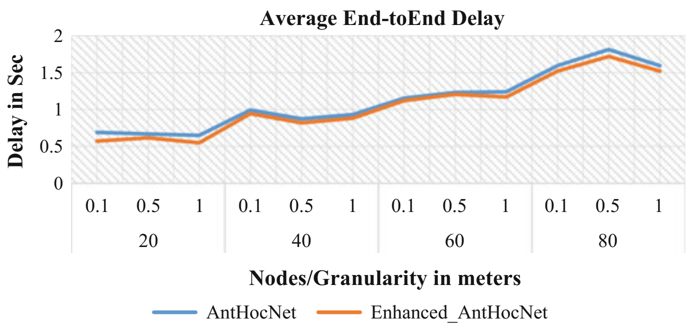


Fig. 6. Average end-to-end delay

Figure 7 shows that the proposed algorithm has shown the significant difference over the traditional AntHocNet with respect to average jitter. In the dense environment (consisting of 80 nodes), the proposed algorithm as less jitter compared to the existing AntHocNet.

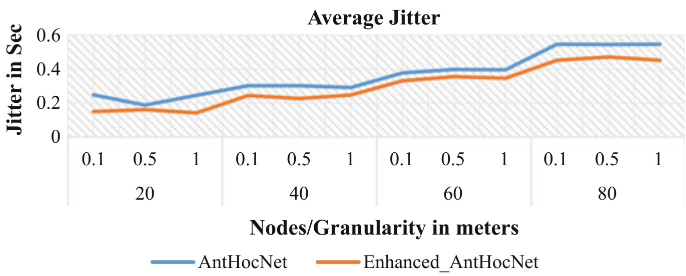


Fig. 7. Average Jitter

5 Conclusion

Vehicular ad hoc networks are particular form of wireless networks formed by vehicles. VANETs comprise vehicles which act as mobile nodes and also routers for other vehicles. Vehicular communication contributes to safer and more efficient roads by providing timely information to drivers and also to make travel more convenient. In this paper, the routing and security aspects of VANETs are addressed. Based on the direction, the paper focused on two cases: (1) destination vehicle moving in same direction as of source and (2) destination vehicle moving in opposite direction to that of source. The performance of the proposed algorithm has been evaluated with existing algorithms; the proposed algorithm has outperformed the existing algorithm with respect to metric number of link failures, end-to-end delay, average jitter, energy consumption, and network lifetime. The observation shows that in the proposed algorithm, there is 18% reduction in link failures compared to the traditional AntHocNet algorithm. With respect to jitter, compared to the existing algorithm, the proposed algorithm has 18.5% reduction and it has less jitter compared to the traditional AntHocNet. There is 6% reduction in the end-to-end delay in the enhanced algorithm. For future enhancement, the velocity of the vehicle can be considered to improvise the performance of the algorithm.

References

1. Namboodiri V, Agarwal M, Gao L, A study on the feasibility of mobile gateways for vehicular ad-hoc networks. In: Proceedings of the first international workshop on vehicular ad hoc networks
2. Wang Y, Fan L, Vehicular ad hoc networks book chapter guide to wireless ad-hoc networks
3. Namboodiri V, Agarwal M, Gao L (2004) A study on the feasibility of mobile gateways for vehicular ad-hoc networks. In: Proceedings of the first international workshop on vehicular ad hoc networks, pp 66–75
4. Ooi C-C, Fisal N (2004) Implementation of Geocast-enhanced AODV-bis routing protocol in MANET. In: Proceedings of the IEEE Region 10 Conference, vol 2, pp 660–663
5. Briesemeister L, Schäfers L, Hommel G (2000) Disseminating messages among highly mobile hosts based on inter-vehicle communication. In: Proceedings of the IEEE intelligent vehicles symposium, pp 522–527

6. Ko Y-B, Vaidya NH (2000) Location-aided routing (LAR) in mobile ad hoc networks. Wireless Netw 6(4):307–321
7. Aquino SR, Arthur E, Robert E, Luke S (2005) Performance evaluation of routing protocols in vehicular ad hoc networks. Int J Ad hoc Ubiquitous Comput 1(1/2) 80–91
8. Perkins CE, Royer EM Ad-hoc on demand distance vector routing. In: Proceedings of the 2nd IEEE workshop on mobile computing systems and applications, pp 90–100
9. Johnson DB, Maltz DA Dynamic source routing in ad hoc wireless networks. In: Imielinski T, Korth HF (eds) Mobile computing. Springer
10. Caro D, Gianni, Frederick D, Luca MG (2005) AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks. European Trans Telecommun 16 (5):443–455