International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Assessing AODV Protocol Suitability for Collision Avoidance Systems

Pratik Kanani[1], Jatinderkumar R. Saini[2]*, Darshana Sankhe[3], Deepali Patil[4], Gayatry Pandya[5], Archana Nanade[6], Bhoomi Shah[7]

Submitted: 24/10/2023 **Revised:** 20/12/2023 **Accepted:** 28/12/2023

Abstract: In Vehicular Ad-hoc Networks (VANETs), the communication is not limited to message transmission but also encompasses the dissemination of crucial information to avert catastrophic incidents. This message exchange occurs through diverse routing protocols, which comprise a predefined set of instructions for both vehicles on the road and stationary vehicles, serving as intermediaries to forward messages to vehicles ahead, known as road-side units (RSU). In this research, our primary focus revolves around the examination and comprehension of the AODV model, recognized for its effectiveness in handling variations in vehicle speed, vehicle density, and average throughput, outperforming other protocols. Specifically, our investigation delves into the performance of the AODV protocol in scenarios where multiple nodes coexist in close proximity, particularly in delivering collision avoidance messages. In high-density vehicular environments, the AODV protocol faces challenges such as broadcast storms and limited link lifetimes, which hinder the successful transmission of collision messages. This paper scrutinizes and translates these phenomena into a mathematical model for further analysis. The traditional AODV protocol demonstrates diminished efficiency in situations where nodes are unreachable, forwarding paths become unstable, link lifetimes are brief, and broadcast storms occur.

Keywords: *AODV, RSU, Collision Avoidance System, Broadcast storm, Packet Delivery fraction, Overhead, Packet Loss*

1. Introduction

Vehicular Ad-Hoc Networks (VANETs) help to understand and simulate the concept of smart vehicles and different technologies pertaining to them. It is an ad-hoc network where several moving vehicles and other devices come in contact with each other via different connecting and communicating measures. Each vehicle and other devices act as a node thereupon acting to transfer data from one vehicle to other vehicles/units on-road facilitating vehicle to vehicle (V2V) data transfer. VANET is primarily used to adhere to the vehicle's driver and the passenger's safety, also improving the efficacy of traffic safety thus making it the key component of the Intelligent Transport System (ITS) [1]. VANET being a sub-part of Mobile Ad-Hoc Network (MANET) creates a pool of mobile networks between the vehicles facilitating the exchange of information. The communication between the vehicles, that acts as a node that contains On-Board Units (OBU's) which is the crux of how information passes, and various parameters pertaining to the vehicle such as speed, position, distance, and inter-vehicular distance.

Taking into account the burgeoning growth of IoT, the field of cloud computing has a set of rules to grow within. The cloud server is not capable enough to keep it on track with the latency requirements of the modern-day application [2]. Considering this, fog computing was introduced by Cisco, in which the technology and the computational ability are far better thereupon leading to a more efficacious system overall. Foreseeing this, the creation of fog computing is sought to be delivering the need in the network access domain by providing reduced latency, better productivity, and optimal usage of bandwidth. A new approach called Vehicular Fog Computing (VFC) is devised which pertains to the theory of seeing vehicles as nodes, VFC aids VANET in basically making up the desired pool of network architecture among the vehicles in its vicinity enabling them to interconnect and help perform communication among each other.

Road Side Units (RSUs) is a radio frequency, high power, and long-range antenna to access a wireless medium. A network stack to run VANET-specific network, link, and physical layer protocols. It is responsible for forwarding data packets to On-Board units (OBU) (present in vehicles) in its range and other RSUs and also the aggregation of safety information from OBUs through safety applications and alarming incoming OBUs. Primarily it works as a gateway to provide Internet connectivity to OBUs.

1.1. Difference between VFC and VANET

VFC distinguishes itself from other existing techniques with its proximity to end-users, dense geographical distribution, and support for mobility [3]. Therefore, VFC exploits the best of the features of slow-moving and parked vehicles, such as clustering distribution in locations, to enable them to collaborate with nearby vehicles to process the data gathered from the vicinity.

Instead of relaying information to a central server, the VFC idea emphasizes additional capabilities such as leveraging nearby vehicle resources and allowing them to cooperate with one

---

[1] *Dwarkadas J. Sanghvi College of Engineering, Mumbai, India*
ORCID ID : 0000-0002-6848-2507
[2] *Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India*
ORCID ID : 0000-0001-5205-5263
[3] *Dwarkadas J. Sanghvi College of Engineering, Mumbai, India*
ORCID ID : 0000-0001-8510-5810
[4] *Dwarkadas J. Sanghvi College of Engineering, Mumbai, India*
ORCID ID : 0000-0001-5835-3237
[5] *Dwarkadas J. Sanghvi College of Engineering, Mumbai, India*
ORCID ID : 0009-0000-7135-0559
[6] *Mukesh Patel School of Technology Management and Engineering, NMIMS University, Mumbai, India*
ORCID ID : 0000-0002-2886-5810
[7] *The Maharaja Sayajirao University of Baroda, Vadodara, India*
ORCID ID : 0000-0001-6881-2919

another. Because one does not have to transport data to remote servers, there is a huge reduction in deployment time and cost. Geo Distribution, local decision-making, and real-time load-balancing are all innovative aspects that set our suggested VFC model apart from the competition.

Pertaining the stationary vehicles or so-called parked vehicles play a crucial role in this sequential method of communication. They act as Road Side Unit (RSUs) [4] and allow navigation of data traffic like sending safety messages across the network. In simpler words, the RSUs jointly act like a Wi-Fi VANET central system and the other vehicles are the access points or in our terminology called nodes that help the entire system access the Internet.

2. Protocols in Vanets

VANET is diversified as it contains several routing protocols, and they are categorised as per their properties, applications, and specifics [2]. Based on the topology routing theory, there are three categories namely

1. Proactive routing protocols
2. Reactive routing protocols
3. Hybrid routing protocols.

Below mentioned are the protocols discussed in a concise manner - DSDV (a proactive routing protocol), DSR, and AODV (on-demand geography-based routing protocols). Further information on several types of routing protocols is to be found in [5].

2.1. Distance sequenced distance vector (DSDV) protocol

DSDV is an example of proactive routing protocol which is a table-driven algorithm that implements the use of routing entry in the table. In the routine discovery phase, the routing information from the source to the destination is procured and updated periodically rather than creating paths for routing packets. The updating process takes place through two methods namely, time-driven and event-driven wherein in the time-driven, there is regular updating of information between the source and destination (nodes and neighbors) whereas in the event-driven there is a trigger-based system due to many numbers changes in the metrics of a particular routing entry. In DSDV, unlike reactive protocols, the availability of paths of all destinations always has a less delay in the set-up process but the main discrepancy here is that this protocol requires constant updates of its routing tables, which drains up the battery and a small amount of bandwidth even when the network is sitting idle.

2.2. Adhoc On Demand Distance Vector (AODV) protocol

It is a topology-based on-demand routing protocol that routes packets from a source to a destination using link information. It acts on nodes in two phases namely Route Discovery and Route Maintenance, using a hopping pattern [5].

- **Route Discovery:** When a sender node in AODV wants to forward a message to a destination node that isn't a neighbor, the sender node utilizes the neighbor to broadcast a Route Request (RREQ) message that contains numerous critical details such as source and destination addresses, as well as the message life cycle. During the route discovery phase, intermediate nodes copy the address of the source node from which the RREQ message originates, while RREQ copies the sequence identities (addresses) of the intermediate nodes at the same time. It keeps going through the network until it reaches the destination node. The Route Reply (RREP) message would be sent to the source node using the stated addresses (prior hops) in the routing database.
- **Route Maintenance:** Each node uses a routing table to keep track of the next destination hop's route. If the links between the intermediate nodes fail, AODV sends a route error message to the source node, indicating that the path to the destination nodes is no longer reachable. A new route-finding process is triggered when this occurs.

2.3. Dynamic Source Routing (DSR) protocol

It is another topology-based reactive routing system that uses a source routing technique, in which the path across intermediary nodes is cached. It has two phases, similar to AODV in terms of hop-by-hop operation. [5]

- **Route Discovery:** This phase duplicates the sequence identities of intermediate nodes that RREQ has passed through, and once it reaches the destination node, the sequences are utilized to send RREP to the source node which includes the complete route taken by RREP. It's worth noting that this has a higher routing overhead than AODV.
- **Route Maintenance:** When the existing path to the target becomes unreachable, alternate routes are used. If there are no other options, a fresh route finding process is launched. The routing cache entries for newly discovered routes would be updated. This technique works well in low-mobility situations because alternate routes are tried before the route discovery step is restarted.

The performance of DSDV, AODV, DSR in an urban street setting is investigated and evaluated. One goal this paper seeks to achieve is how these three routing methods function when stationary and moving cars on a city street exchange TCP traffic in order to enable VFC infrastructures. To begin, road maps are created using Open Street Map (OSM), a map editing application that allows real-world locations to be extracted into an OSM or osm.xml file. The road map is then imported into SUMO (Simulation of Urban MObility), an open-source, highly portable, microscopic, and continuous traffic simulation package designed to handle large networks, which generates the necessary tcl script and mobility trace files. Finally, the VANET scenario is simulated using NS-2, a network simulator, in order to evaluate the performance of the aforementioned reactive routing protocols. Based on SUMO mobility traces, this paper successfully conducted performance simulation and evaluation of DSDV, AODV, and DSR routing protocols under various vehicle densities, parking durations, and vehicle speeds. The conclusion of this article is that AODV outperforms the other routing methods. [5]

3. Literature Review

AODV is a routing protocol chosen for specific network scenarios due to its intrinsic characteristics that make it particularly well-suited for certain applications. One of the primary reasons for the selection of AODV is its dynamic nature [6], which makes it ideal for networks characterized by frequent topology changes. In highly dynamic networks, where nodes constantly join or leave the network, AODV's reactive approach allows for on-demand route discovery. This ensures that routes are established as needed, optimizing resource usage and adaptability to changing network conditions.

Moreover, AODV exhibits a stable packet delivery ratio in dynamic networks [6-7], especially where on-demand routes can be established efficiently. This stability is essential in scenarios where the quality of service and reliable data transmission areparamount. AODV's ability to maintain a consistent packet delivery ratio contributes to the protocol's preference in applications with dynamic and challenging network conditions.

Scalability is another factor favouring AODV, particularly in larger networks [8]. The on-demand route establishment characteristic of AODV helps mitigate the scalability challenges often encountered in expansive networks. The protocol's efficient utilization of resources in establishing routes as needed promotes its suitability for larger-scale deployments, ensuring effective communication in such environments.

AODV's adaptability to variable network conditions [9] is a crucial attribute. In unpredictable network environments, AODV's reactive approach enables it to quickly respond to changes, allowing for efficient route adjustments as the network topology evolves. This adaptability is vital in applications where network stability and responsiveness to fluctuations in conditions are essential, further justifying AODV's selection in such contexts.

AODV is particularly well-suited for several application scenarios, where its specific characteristics align with the requirements and challenges of these environments. Firstly, in Mobile Ad Hoc Networks (MANETs), AODV shines due to its on-demand nature and adaptability [6]. MANETs involve nodes that frequently change their positions, and AODV's ability to establish routes only when necessary and adapt to changing topologies is highly beneficial for these networks.

Secondly, AODV finds favour in Wireless Sensor Networks (WSNs) [7], where resource constraints are a concern. AODV's efficiency in establishing routes on-demand ensures minimal resource utilization, a critical factor in energy-constrained sensor networks.

In the domain of emergency and disaster response [9], AODV's quick adaptability to changing network topologies is invaluable. In such scenarios, communication infrastructure may be disrupted or rapidly reconfigured, and AODV's ability to establish routes as needed supports efficient and resilient communication during emergency situations.

Vehicular Ad Hoc Networks (VANETs) [10] represent another area where AODV is advantageous. VANETs are inherently dynamic, with vehicles entering and leaving the network frequently. AODV's reactive approach aligns well with the on-road dynamics, allowing for efficient route establishment in these highly dynamic environments.

Lastly, in military and tactical communication networks [11], AODV's adaptability and the ability to establish routes on-demand are crucial. Military operations often take place in dynamic and unpredictable environments, and AODV's responsiveness to changes ensures reliable and flexible communication infrastructure.

AODV, while offering various advantages, is not without its challenges. These challenges must be considered in the selection and deployment of the protocol:

Firstly, the route discovery process in AODV can result in increased control message overhead in the network [6]. When a route is not available, AODV initiates a route discovery process, which involves flooding the network with route request messages. This overhead can impact the efficiency and bandwidth utilization of the network, particularly in scenarios with frequent route discoveries.

Scalability issues can also arise, particularly in very large networks or networks with high mobility [12]. AODV's proactive approach to route maintenance and its reliance on maintaining routing tables for all nodes can become impractical in large-scale deployments. The continuous updates and maintenance of routing information can lead to scalability challenges.

Route maintenance overhead is another challenge [7]. In dynamic networks, frequent changes in the network topology may result in more frequent route maintenance messages, such as route error messages. This increased overhead can affect the network's performance and consume valuable resources.

Security concerns are inherent in AODV [13]. The protocol may be susceptible to various security threats, including packet spoofing, route manipulation, and denial of service attacks. Protecting AODV against such threats is a critical aspect of its deployment, and security mechanisms are necessary to ensure the integrity and authenticity of routing information.

Moreover, AODV's adaptability [14], while generally advantageous, may face challenges in scenarios with rapid and frequent topology changes. Adapting to such changes can introduce additional complexity and potentially impact the stability of the network, necessitating careful network management and optimization.

A Collision Avoidance System (CAS) is a safety technology designed to prevent or mitigate collisions between vehicles, pedestrians, or other obstacles. CAS typically employs various sensors, radar, LIDAR, cameras, and communication systems to monitor the surrounding environment and provide warnings or take autonomous actions to avoid collisions.

Collision Avoidance Systems are fundamental components of communication networks, playing a pivotal role in ensuring efficient and reliable data transmission. These systems are crucial for various reasons:

Efficient medium access is one of the primary benefits of CAS. CAS mechanisms optimize the way devices access the communication medium, ensuring that multiple devices can transmit data without interfering with each other. This optimization is critical for reducing contention and enhancing the overall network's efficiency. [15]

Enhanced throughput is another vital aspect of CAS. By preventing collisions and minimizing retransmissions, CAS mechanisms contribute to increased throughput in communication networks. This efficiency is especially essential in scenarios where high data transfer rates are required [16].

In wireless networks, CAS is crucial for ensuring reliable communication. Wireless environments are susceptible to interference and contention, making collision avoidance mechanisms vital for reducing the likelihood of data corruption and packet loss. CAS ensures that data packets are transmitted and received correctly, enhancing the reliability of wireless communication [17].

Quality of Service (QoS) improvement is a significant outcome of CAS implementation. CAS mechanisms minimize delays, reduce packet loss, and ensure timely delivery of data packets. This results in an improved user experience, particularly in applications where QoS is a critical factor [15].

CAS also contributes to network stability by preventing excessive collisions, which can lead to congestion and performance degradation. Network stability is essential for maintaining a reliable and consistent communication environment, making CAS indispensable in this regard [17].

The integration of AODV (Ad Hoc On-Demand Distance Vector) routing protocol and CAS holds significant potential in enhancing the safety and efficiency of communication networks, particularly in vehicular environments like Vehicular Ad Hoc Networks (VANETs). This integration offers several benefits and presents certain disadvantages:

The integration can lead to enhanced safety awareness among vehicles in a VANET. By exchanging safety-related information through the AODV routing protocol, vehicles can gain real-time insights into potential collision risks and safety-critical events, thus improving overall safety awareness. This heightened safety awareness is invaluable for reducing accidents and improving road safety.

Optimized route selection for safety is another advantage of integrating AODV and CAS. CAS data, such as real-time collision warnings and hazard notifications, can influence AODV's route selection algorithm. This means that the routing protocol can prioritize routes that minimize collision risks or provide safe paths to vehicles. By doing so, the integration enhances the safety of vehicle-to-vehicle communication in VANETs.

Efficient traffic management is facilitated through this integration. CAS information can be used to optimize AODV routing decisions, resulting in more efficient traffic management. By considering real-time data on traffic conditions, road hazards, and vehicle speeds, AODV can route traffic more effectively, reducing congestion and improving the overall flow of vehicles in the network. Coordinated collision avoidance is made possible through the integration of AODV and CAS. Vehicles can collaborate based on AODV-derived routes and CAS warnings to implement coordinated collision avoidance strategies. This collaborative approach can significantly reduce the risk of accidents and collisions, enhancing overall safety in VANETs.

Furthermore, the integration allows for dynamic adaptation to changing network conditions. AODV is known for its ability to adapt dynamically to variations in the network topology, and CAS data can influence routing decisions in response to real-time safety conditions. This adaptability ensures that the network remains responsive and robust, even in rapidly changing traffic and environmental conditions.However, this integration does present certain challenges and disadvantages:

Increased network overhead is a potential challenge [18]. The exchange of safety-related information and frequent route updates driven by CAS can introduce additional network traffic. This increased overhead may impact the efficiency and bandwidth utilization of the AODV protocol, potentially leading to congestion and reduced network performance.

Security concerns arise when integrating safety-related information into the routing protocol [18]. Ensuring the authenticity and integrity of CAS data becomes critical, as malicious or false information injected into the network can lead to incorrect routing decisions and safety hazards. Implementing robust security mechanisms is essential to mitigate these risks.

Scalability issues may be a concern, particularly as the number of vehicles in the VANET increases [18]. Processing and disseminating large volumes of CAS data and route updates to a growing number of vehicles can strain the network's resources. Mitigating scalability challenges may require the exploration of optimization techniques and distributed approaches to handle the increasing load efficiently.

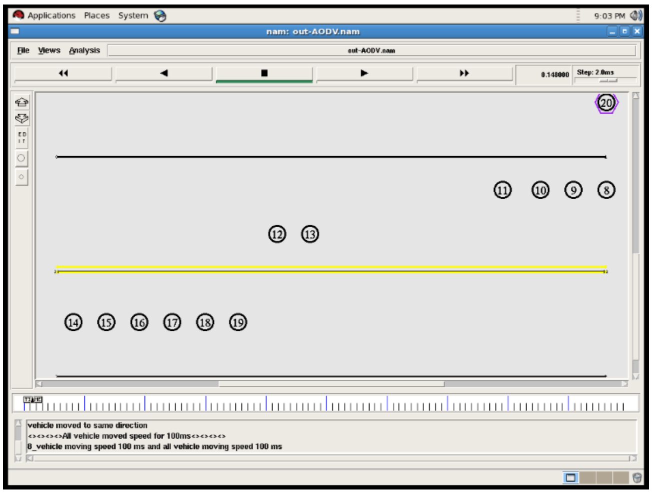
In conclusion, the integration of AODV and CAS offers substantial benefits in terms of safety and efficiency in VANETs. Still, careful consideration must be given to the potential challenges, such as network overhead, security, and scalability, to ensure that the advantages of this integration are maximized while addressing its limitations.

4. Implementation

The numbered circles represent the vehicles (nodes), the numbers encircled within a hexagon represent an RSU. The two-way path between the black lines is the road which is divided by a divider in yellow color. As shown in the figures below, the concentric lines around the RSU describe its permissible range.

4.1. Simulation Setup

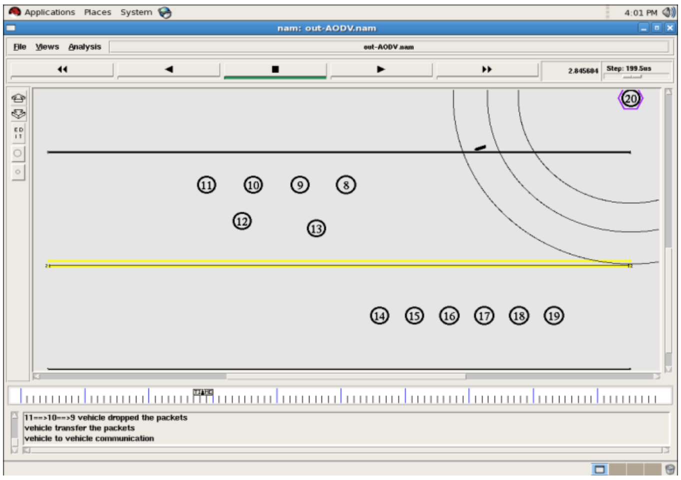
Further working on AODV, a simulation on NS-2 displays the basic packet transfer route using the AODV protocol. The hypothetical setup created (refer figure 1) includes RSU and moving vehicles as well as initially parked vehicles. All the vehicles move in their respective directions and are not expected to change direction during the course of the simulation. The simulation records factors like packet delivery factor, packet overhead, and packet loss and presents them in a graph for a better perception of the protocol.



```
vehicle moved to same direction
<><><><>All vehicle moved speed for 100ms<><><><>
8_vehicle moving speed 100 ms and all vehicle moving speed 100 ms
```

Fig. 1. Environment setup of the simulation

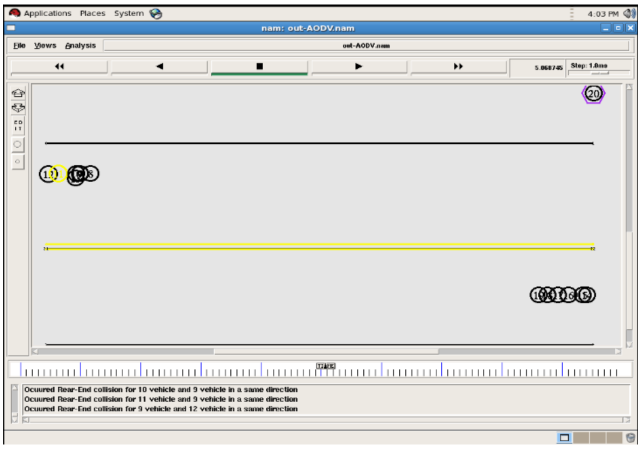
Our scenario consists of a two-way street wherein the yellow line acts as a divider. Initially, two sets of cars on either side of the road (4 and 6 respectively) start moving in a straight path opposite to each other with the 20th node acting as an RSU, vehicles 12 and 13 (fig 1) act as parked vehicles in our simulation which join the other vehicles as the simulation proceeds. Each vehicle moves at a speed of 100ms. The 8th vehicle which initially receives the packet from the RSU then transmits it to the vehicles in front of it. This happens until a point after which the nodes (9,10,11) start dropping packets. This happens due to a phenomenon called a broadcast storm which is pondered upon later in the paper.



11==>10==>9 vehicle dropped the packets
vehicle transfer the packets
vehicle to vehicle communication

Fig. 2. RSU sending a message to vehicle

As the simulation proceeds, vehicles 12 and 13 join the other vehicles with a speed of 100ms. The route for packet transfer still remains the same. There is no direct communication between vehicles 12 and 10,9 or 8 similar is the case with vehicle 13. Vehicles 12 and 13 then start moving in the same direction as the other vehicles until the 11th vehicle approaches the danger zone (a region where accidents are anticipated in the simulation ie. the leftmost region of the first lane).



Ocuured Rear-End collision for 10 vehicle and 9 vehicle in a same direction
Ocuured Rear-End collision for 11 vehicle and 9 vehicle in a same direction
Ocuured Rear-End collision for 9 vehicle and 12 vehicle in a same direction

Fig. 3. Failure of AODV causing a collision of vehicles

Figure 3 depicts a scenario where traditional AODV fails to communicate emergency messages to the vehicles involved and this, in turn, leads to collisions among vehicles. The 11th vehicle enters the danger zone and stops. In an ideal case, the collision avoidance system should trigger an emergency message which would then notify the 12th vehicle (the one immediately following the 11th vehicle) that the vehicle ahead has stopped. However, this is not what happens. Because radio signals are likely to overlap with those of others in a geographic area, broadcasting by floods is usually very expensive and results in significant redundancy, conflict, and collision, which we refer to as the broadcast storm problem [19]. A broadcast storm in the network disrupts the communication system because of which the 12th vehicle is unaware of the state of the 11th vehicle. This results in multiple rear-end collisions between vehicles. Figure 3 above makes a case for the collision between vehicles 10 and 9, 11 and 9, 9 and 12.

5. Understanding The Working Of VFC Model, AODV Protocol And QoS Parameters

The entire scenario can be expressed using the following equations

5.1. Mathematical Model of Vehicular Fog Computing (VFC):

$$Vehicle\_Fog=\sum_{V_{fog}=1}^{n} nn(\text{number of nodes})\text{.................}1$$

$$Vehicle\_Fog\_xloc = \sum_{V_{fog}=1}^{n} x(i)\ldots\ldots\ldots(x \text{ is 'location of fognodes'}))\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.2$$

$$Vehicle\_Fog\_yloc = \sum_{V_{fog}=1}^{n} y(i)y \ldots\ldots\ (y \text{ is 'location of fog nodes'})\text{.....................}3$$

Now, to initialize fog nodes in this vehicular network the equations are as follows:

$$Vehicle\_Fog\_init = \sum_{V_{fog}=1}^{n}(N_n(n_1)(n_2)(n_3)\ldots\ldots(n_n)\ldots\ldots(y \text{ is 'location of fog nodes'})$$

In the above equation, N_n is the number of Fog created in this network n_1 is node 1 upton_n which represents node$_n$.

Seeing the current location of each fog node in this vehicular network from the equation 2 and 3, which is the Vehicle_Fog_xloc and Vehicle_Fog_yloc respectively.

The On-Board units (OBU) present in the vehicles are used to compute these parameters.

$$Node\_Current\_loc = \sum_{V_{fog}=1}^{n}(Vehicle\_Fog\_xloc * Vehicle\_Fog\_yloc)$$

$$Loc = \sum_{V_{fog}=1}^{n} Fog\ (xx_i, yy_j)\ldots\ldots\ldots.4$$

Initially, all fog nodes are placed in one location, during the communication time fog nodes displacement from initial location to target location to target location.

Now, let us see the mobility of the fog nodes from the below equation

$$Mobility=\sum_{V_{fog}=1}^{n}(Vehicle\_Fog\_Speed*distance)\text{..............}5$$

Using the two overheads added i.e distance and speed it is possible to trace the current location of the vehicles which is then used by the AODV protocol for route selection.

5.2. Ad-Hoc on demand distance vector routing protocol

```
Begin
$RREQ = \sum_{V_{fog}=1}^{n}(\text{sends RREQ packet to all its neighbors})$……………………………………………..….6
A source requires sending a message to destination
    if (source $\sum_{V_{fog}=1}^{n}$(does not have valid route) )
        puts (source initiates route discovery process)
Identifying route request of every node
$Ide\_RREQ = \sum_{V_{fog}=1}^{n} [b\_id, IP\_id]$……… … ….…..… … … … … 8
In the above equation 8,
$\sum_{V_{fog}=1}^{n} \rightarrow RReply, b_{id} \rightarrow broadcast_{Id},$
$\sum_{V_{fog}=1}^{n} IP\_add \rightarrow IP\ address$
if (route contains (AODV))
    begin
    $Vehicular\_Fog\_AODV = \sum_{V_{fog}=1}^{n}(\text{Route request and Route reply})$........................................................................9
    end
End
```

1. In this Vehicular Fog Computing (VFC), provides the security in fog computing environment. Initially, all the vehicles move towards the target location according to road side unit (RSU)

$$Mobility = \sum_{V_{fog}=1}^{n} (Vehicular\_Fog\_mobility * distance)$$

2. To generate and update the anonymity of vehicles and reduce the time of authentication with legitimate vehicles and RSUs. In this simulation, we implemented selective path forwarding for an optimal secure route in AODV.

```
if (route contains (AODV))
    begin
    $Vehicular\_Fog\_AODV = \sum_{V_{fog}=1}^{n} (r_{req} + r_{rep})$
end
end
```

5.3. QoS parameters

From the above given equation, result parameter has been analyzed and calculated using the formula, is given below:

1. **Packet Delivery Fraction**: it is the ratio of number of packets successfully received to the total number of packets sent

$$VRPF\_PDF = \frac{\sum_{packets=1}^{n} successfully\ received\ packets}{\sum_{packets=1}^{n} total\ sent\ packets}$$

2. **Overhead**:

$$VRPF\_Overhead = \frac{\sum_{packets=1}^{n} rt\ packets}{\sum_{packets=1}^{n} data\ packets}$$

3. **Packet Loss Ratio:**

$$VRPF\_PLR = \frac{(\sum_{packets=1}^{n} lost\ packets)}{\sum_{packets=1}^{n}(rx\ packets + lost\ packets)}$$

6. Results and Discussions

An exponential increase in the overhead packets in a very minimal amount of time is observed due to broadcast storm and then it consistently decreases as the network becomes ineffective.

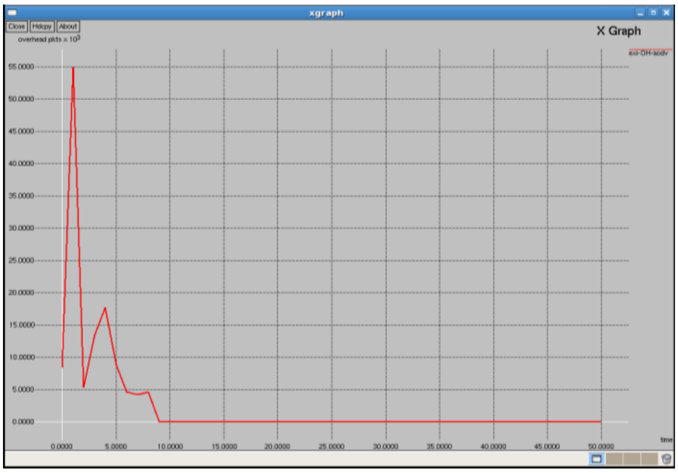


Fig. 4. Overhead vs Time

At increased vehicle density, AODV, which is a reactive routing protocol, there is a frequent rise in route discovery activities to establish routing with newer surrounding nodes, resulting in larger routing overhead which is the main reason for initiation of broadcast storm.

As seen in Fig 5, there is an exponential increase in the loss which directly affects the sustainability of the network. Losing packets of data infers that the message is not delivered or not delivered completely, both of which can cause collisions and make the network ineffective. This loss mainly occurs because the networks get flooded with route discovery packets which leads to multiple collisions.

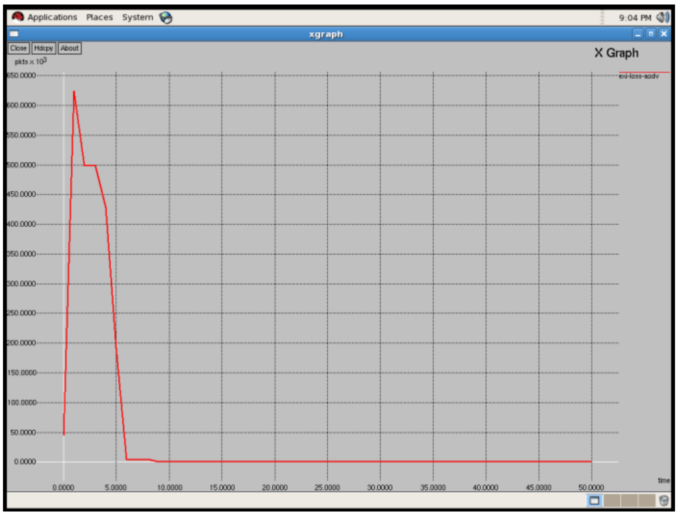


Fig. 5. Loss vs Time

In a relatively short period of time, exponential growth in the packet delivery factor is observed, which then steadily diminishes.

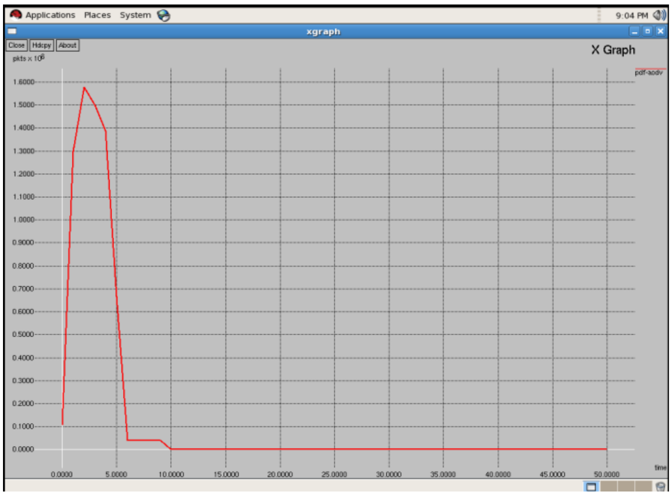


Fig. 6. Packet delivery factor vs Time

Because AODV is a reactive routing protocol, there is a frequent increase in route discovery operations to establish routing with newer surrounding nodes as vehicle density rises, resulting in higher routing overhead.

7. Conclusion

In this research paper, we have conducted an in-depth examination of the AODV protocol and its utilization within the context of VANET (Vehicular Ad Hoc Networks). Our investigation encompasses various aspects, including the rationale for adopting the AODV protocol, its optimal applications, and the associated challenges. We have also underscored the significance of a Collision Avoidance System (CAS) in the context of VANET. Upon attempting to implement CAS using the AODV protocol, we encountered a notable disparity in its performance compared to other protocols commonly used in VANET. Multiple Roadside Units (RSUs) were deployed, leading to the occurrence of a broadcast storm. Consequently, the reliable delivery of packets to their intended destinations became a considerable challenge. This was evident in our testing results, specifically in the packet delivery ratio, where a sudden drop in the number of successfully delivered packets was observed. Additionally, our packet loss graph depicted a rapid decline as the network's lifetime neared its end due to the overwhelming volume of packet transmissions. The packet overhead reached its peak and subsequently dwindled to near-zero levels. Collectively, these observations signify a pressing need for further improvements in the AODV protocol to facilitate the successful implementation of CAS.

We have also carried out mathematical analyses of these phenomena, shedding light on the areas requiring enhancement within the protocol. This research paves the way for further investigations aimed at refining the AODV protocol for optimal performance in CAS applications within VANET.

Author contributions

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by all authors. The manuscript was written and revised by all authors on previous versions of the manuscript. All authors read and approved the final manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Safi, Q. G. K., Luo, S., Pan, L., Liu, W., Hussain, R., & Bouk, S. H. (2018). SVPS: Cloud-based smart vehicle parking system over ubiquitous VANETs. Computer Networks, 138, 18-30. https://doi.org/10.1016/j.comnet.2018.03.034

[2] Byers, C.C. (2017). Architectural Imperatives for Fog Computing: Use Cases, Requirements, and Architectural Techniques for Fog-Enabled IoT Networks. IEEE Communications Magazine, 55, 14-20.

[3] Raut, Swati & Malik, Latesh. (2014). Survey on vehicle collision prediction in VANET. 10.1109/ICCIC.2014.7238552.

[4] Yeferny, Taoufik and Sabri Allani. “MPC: A RSUs deployment strategy for VANET.” International Journal of Communication Systems 31 (2018): pp. 1043-1052.

[5] Yura, A., Newaz, S., Rahman, F. et al. Evaluating TCP performance of routing protocols for traffic exchange in street-parked vehicles based on fog computing infrastructure. J Cloud Comp 9, 18 (2020). https://doi.org/10.1186/s13677-020-00159-w

[6] C. Perkins and E. Royer, "Ad-hoc On-Demand Distance Vector Routing," in IEEE Transactions on Mobile Computing, vol. 2, no. 4, pp. 353-363, Oct.-Dec. 2003, doi: 10.1109/TMC.2003.844091.

[7] M. Marina and S. Das, "Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks," in Proceedings of the 2001 IEEE International Multitopic Conference (INMIC), Lahore, Pakistan, 2001, pp. 122-126, doi: 10.1109/INMIC.2001.996481.

[8] Z. Haas and M. Pearlman, "Zone Routing Protocol (ZRP): A Hybrid

Routing Approach for Ad Hoc Networks," in IEEE Transactions on Mobile Computing, vol. 1, no. 1, pp. 11-18, Jan.-Mar. 2002, doi: 10.1109/TMC.2002.1027544.

[9] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," in Proceedings of INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies, Kobe, Japan, 1997, pp. 1405-1413, doi: 10.1109/INFOCOM.1997.635515.

[10] M. Raya and J.-P. Hubaux, "Vehicular Ad Hoc Networks: A New Challenge for Communication Technology," in IEEE Communications Magazine, vol. 46, no. 11, pp. 136-144, Nov. 2008, doi: 10.1109/MCOM.2007.4297419.

[11] B. Adamson et al., "Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations," RFC 2501, DOI: 10.17487/RFC2501.

[12] Y. Zhang and W. Lee, "A Performance Comparison of Proactive and Reactive Routing Protocols for Mobile Ad Hoc Networks," in Proceedings of the 19th International Conference on Distributed Computing Systems Workshops (ICDCSW '99), Austin, TX, USA, 1999, pp. 730-735, doi: 10.1109/ICDCSW.1999.776991.

[13] N. Saxena and P. Gupta, "Security Attacks and Solutions in Mobile Ad-Hoc Networks: A Review," in 2017 IEEE Calcutta Conference (CALCON), Kolkata, India, 2017, pp. 28-32, doi: 10.1109/ICCS.2017.8280921.

[14] E. M. Royer and C. E. Perkins, "Performance Comparison and Analysis of Table-Driven and On-Demand Routing Protocols for Ad Hoc Networks," IEEE STD 802.11, 1999, pp. 180-188, doi: 10.1109/IEEESTD.1999.790941.

[15] M. A. Hoque and H. Hassanein, "A survey on medium access control protocols for vehicular ad hoc networks," in Computer Networks, vol. 108, pp. 67-85, Jan. 2016, doi: 10.1016/j.comnet.2016.11.019.

[16] X. Cheng, W. Cheng, and H. Chen, "Analysis of Carrier Sense Multiple Access with Collision Avoidance Protocols in Vehicular Ad Hoc Networks," in Journal of Sensors, vol. 2016, Article ID 9459082, 2016, doi: 10.1155/2016/9459082.

[17] M. Tawalbeh, A. Khreishah, J. Kang, and K. A. Harras, "Collision Avoidance Techniques for IEEE 802.11 Wireless Networks: A Survey," in IEEE Access, vol. 5, pp. 18414-18443, 2017, doi: 10.1109/ACCESS.2017.2760038.

[18] A. Naik, S. M. Shendge, and V. T. Gaikwad, "A survey of collision avoidance systems and technologies," in International Journal of Vehicular Systems, vol. 2014, Article ID 59680, 2014, doi: 10.1504/IJVS.2014.059680.

[19] Ni, Sze-Yao & Tseng, Yu-Chee & Chen, Yuh-Shyan & Sheu, Jang-Ping. (1999). The Broadcast Storm Problem in a Mobile ad hoc Network.. Wireless Networks. 8. 151-162. 10.1145/313451.313525.