iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IV **Month of publication:** April 2022

DOI: https://doi.org/10.22214/ijraset.2022.41559

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IV Apr 2022- Available at www.ijraset.com

Networking in Vehicular Ad-Hoc Networks (VANET) for Accident Prevention

Pascoal Daniel Fernandes[1], Dr. M. N. Nachappa[2]
[1]*M. Sc. I. T. Student, Jain (Deemed-to-be) University, Karnataka, India.*
[2]*Dean School of CS & IT, Jain (Deemed-to-be) University, Karnataka, India.*

Abstract: ***VANET (Vehicular Ad Hoc Network) is an emerging technology for intelligent inter-vehicle communications. It is a specialized derivation of pure multi-hop ad hoc networking that is currently undergoing industrial prototyping; however, the dreamed idea of a general purpose vehicular ad hoc network is still a long way off. For the past few years, vehicular communication has been a hot topic. The VANET objective is to use short-range wireless technology to provide road safety and commercial comfort applications. Many routing protocols have been designed specifically for such networks, with the majority of them attempting to make use of information that may be available at the vehicle by the time a routing choice is required. We have investigated the AODV and GPSR in this study.***
Keywords: AODV, GPSR, Vehicular Ad Hoc Networks, Ad-Hoc Routing, Routing Protocols.

I. INTRODUCTION

[4] Although the Vehicular Ad-hoc Network (VANET) is not a new topic, it continues to present new challenges and research problems. The main objective of VANET is to help a group of vehicles create and maintain a communication network between them without using a central base station or controller. One of the main applications of VANET is in critical medical emergencies where there is no infrastructure while transmitting information is essential.to save lives. However, with these useful applications of VANET, new challenges and problems emerge. The lack of infrastructure in VANET places additional responsibilities on vehicles. Each vehicle is part of the network and also manages and controls the communication on that network as well as your communication needs. VANET is a variant of MANET (Mobile Ad-hoc NETwork). MANET consists of nodes that communicate without a core network and in which the nodes are equipped with network capabilities. VANET, on the other hand, has proven to be a challenging and more responsible class or variant of MANET. to enter or exit the network in VANET calls for routing protocols other than MANET.

A. VANET Architecture

The VANET architecture is a communication architecture in which the types of communication are characterized in 4 sections, which are summarized as:

1) *Vehicle-to-vehicle Communication (V2V):* The exchange of data between different vehicles to support the driver by informing him about warnings and other critical information among each other. V2V communication does not depend on a fixed infrastructure for data exchange and dissemination., Safety and Protection Applications.
2) *Vehicle-to-Infrastructure Communication (V2I):* This communication that takes place between mobile vehicles and fixed infrastructure on the road to collect data. Provides updates related to environment detection and monitoring, e.g., Real-time traffic updates or weather updates.

B. Characteristics of VANET

The following characteristics define VANET:

1) *High Dynamic Topology:* Vehicles' speed and direction change constantly, resulting in a high dynamic topology.
2) *Intermittent Connectivity:* Device connectivity fluctuates a lot, for example, a link between two devices exchanging information can go down at any time. The high dynamic topology is the cause of frequent disconnection.
3) *Mobility:* Fixed RSUs and moving vehicles make up the majority of VANETs. The vehicle's speed ranges from extremely slow to extremely fast, posing additional communication issues. Indeed, in congested places, vehicles are halted or going slowly, giving them ample opportunity to exchange messages. However, due to the high density of vehicles, they face significant hurdles such as data collision, channel fading, message dropping, and other interference issues. Vehicle speed is extremely high

in low-traffic areas, resulting in various communication issues such as a limited communication window, link failures, and a long end-to-end delay, among others.

4) *On-board Sensors:* The VANET implies that nodes are rarely equipped with on-board sensors capable of transmitting data to other devices or nodes.
5) *Traffic Density:* Depending on the geographic location (i.e., high traffic density in metropolitan areas and low traffic density in rural areas and highways) and the time component, it ranges from high to low density (i.e., low traffic density during off-peak hours and high traffic during rush hours). The creation of efficient VANET communication protocols is complicated by the high volume of traffic. Data distribution techniques must, for example, deal with network disconnection in remote locations with low traffic density. Advanced data transmission systems, on the other hand, should be employed to avoid the well-known broadcast storm problem in cases of high traffic density, particularly in urban areas during peak hours.

C. Components in VANET

[3]The following components used in VANETs are:

1) *Road-Side Units (RSU):* The roadside unit is a computing device that is installed alongside the road or in a specific location, such as a parking lot or a crossroads, to give local connectivity to passing vehicles. The RSU is made up of network devices that use IEEE 802.11p radio technology to provide dedicated short-range communication (DSRC). RSUs, in particular, can communicate with other network devices within other infrastructure networks.
2) *Application Unit (AU):* An AU is a dedicated device that can be a built-in portion of a vehicle or a standalone device like a smartphone or laptop. It can execute a single or multiple apps that take advantage of the OBU's communication capabilities.
3) *On-Board Unit:* In the Vehicular Ad Hoc Network (VANET), the On-Board Unit (OBU) is a unit that enables vehicle-to-vehicle (V2V) communication. The central control module, wireless communication module, GPS module, and human-machine interface module are the four components of the system.

D. VANET Domains

The goal of the VANET is to allow vehicles in close proximity to communicate with one another. The entities in a VANET can be separated into three domains according to IEEE 1471-2000 and ISO/IEC 42010 rules.

1) *Mobile Domain:* The mobile domain is divided into two sections. The first is the vehicle domain, which includes any vehicles that are always moving, such as buses, cars, and trucks. The second domain is the mobile device domain, which includes all portable devices such as PDAs, laptops, GPS, cellphones, and so on.
2) *Infrastructure Domain:* There are two parts to the infrastructure domain. The roadside infrastructure domain includes stationary roadside elements such as traffic lights, poles, and other structures. The central infrastructure domain, on the other hand, includes the central management centres such as vehicle management centres, traffic management centres, and so on.
3) *Generic Domain:* Internet infrastructure and private infrastructure are included in the generic domain. Different nodes, servers, and other computer resources that work directly or indirectly for a VANET, for example, fall within the generic domain.

The mobile domain communicates and exchanges data with the infrastructure domain, which analyses data and performs its own modulation. The infrastructure domain then talks with the generic domain and shares information with it in the second stage. This data flow between stationary and mobile resources allows users to make more efficient and productive use of the route.

E. Routing Protocols

1) *Ad-hoc On-Demand Distance Vector (AODV):* Ad-hoc On-Demand Distance Vector (AODV) is a loop-free routing protocol for ad-hoc networks. It is intended to be self-starting in a mobile node environment, withstanding a wide range of network behaviors such as node mobility, link failures, and packet losses. AODV keeps a routing table at each node. A destination's routing table entry contains three essential fields: a next hop node, a sequence number, and a hop count. All packets with a destination address are routed to the next hop node. The sequence number serves as a form of time stamping and is a measure of a route's freshness. The hop count represents the current distance from the source node to the destination node. Nodes in AODV discover routes through request-response cycles. By broadcasting an RREQ message to all of its neighbours, a node requests a route to a destination. When a node receives an RREQ message but does not have a route to the requested destination, the RREQ message is broadcast. It also remembers a reverse-route to the requesting node, which it can use to forward subsequent responses to this RREQ. This procedure is repeated until the RREQ arrives at a node with a valid route to the destination. This node (which may or may not be the destination) responds with an RREP message. This RREP is unicast through the

intermediate nodes' reverse-routes until it reaches the original requesting node. As a result, at the end of this request-response cycle, a bidirectional route between the requesting node and the destination is established. When a node loses connection to its next hop, it invalidates its route by sending an RERR to all nodes that may have received its RREP.

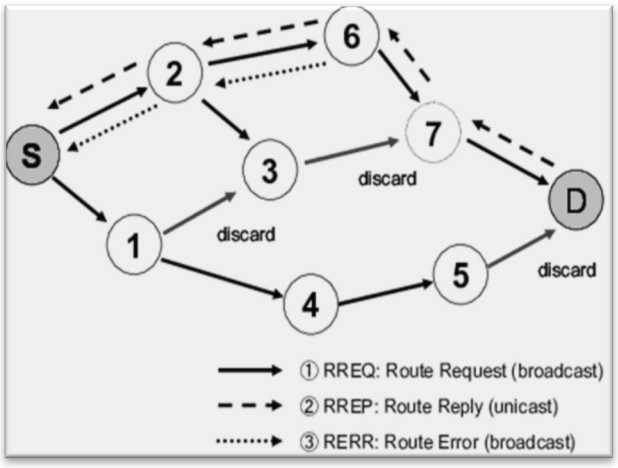


Fig.1. Diagram of AODV Routing Protocol

2) *Greedy Perimeter Stateless Routing (GPSR):* The routing problem of finding paths from a traffic source to a traffic destination through a series of intermediate forwarding nodes is especially difficult in wireless networks with many mobile stations. When nodes move, the network's topology can change quickly. Such networks necessitate a responsive routing algorithm that quickly finds valid routes as the topology changes and old routes fail. However, due to the limited capacity of the network channel, efficient routing algorithms and protocols that do not cause the network to become congested as they learn new routes are required. The mobile routing problem is defined by the conflict between these two goals, responsiveness and bandwidth efficiency. GPSR, or Greedy Perimeter Stateless Routing, is a fast and efficient routing protocol for mobile and wireless networks. Unlike previous routing algorithms, which used graph-theoretic notions of shortest paths and transitive reachability to find routes, GPSR takes advantage of the correspondence between geographic position and connectivity in a wireless network by using node positions to make packet forwarding decisions. GPSR employs greedy forwarding to route packets to nodes that are progressively closer to the destination. In network regions where such a greedy path does not exist (i.e., the only path requires moving temporarily farther away from the destination), GPSR recovers by forwarding in perimeter mode, in which a packet traverses successively closer faces of a planar subgraph of the full radio network connectivity graph until reaching a node closer to the destination, where greedy forwarding resumes.

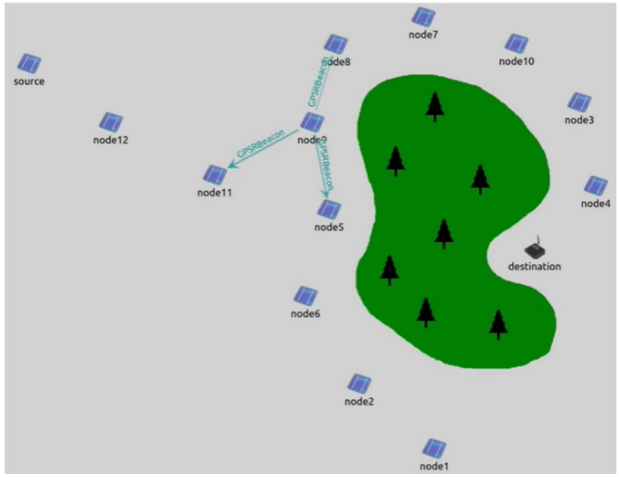


Fig.2. Diagram of GPSR Routing Protocol

GPSR beacons are sent out by the nodes (and learning about the positions of their neighbors). After then, the source sends a ping request packet. It is transmitted through the chain to node 9, which transmits it to node5 since it is the closest neighbor to the target among node 9's neighbors. However, because node5 has no neighbors closer to the destination (and is out of range of the destination), the packet is switched to perimeter mode. The ping packet is sent in accordance with the right-hand rule. The packet reaches node 1 and then loops back up the chain through node 9. Then node10 returns it to greedy routing mode since it is closer to the target than node 5, which was converted to perimeter mode. The package then arrives at its destination. Because the destination is closer to the source than the destination's lone neighbor, node 4, the reply packet begins in perimeter mode. Because it is closer to the source than the destination, the packet is switched back to greedy mode at node 10. It then makes its way to the source through nodes 9 and nodes 11.

II. SYSTEM DESIGN & IMPLEMENTATION

In order to simulate between GPSR and AODV, simulation programs are written and available.

A. Functional Requirements

The requirements to run the simulation are as follows:

1) System requirements.
- Intel(R) Core (TM) i5-10210U CPU @ 1.60GHz 2.10 GHz.
- 8.00 GB RAM.
- 120 GB Internal SSD.

2) Application requirements.
- Microsoft Windows 10.
- [5] OMNET++ Network Simulator.
- INET Framework (VANET Plugin for OMNET++)
- Python 3.4.
- Total 12 GB Space required for building the simulator.

B. Non-Functional requirements

1) Understanding of how simulator works.
2) Understanding the working of AODV Protocol.
3) Understanding the working of GPSR Protocol.

C. Scenarios

Evaluation of different scenarios are based on: -

1) Routing Protocols used:
- AODV: - Ad hoc On-Demand Distance Vector.
- GPSR: - Greedy Perimeter Stateless Routing.

2) The Densities of vehicles:
- Low: - 10 vehicles.
- Medium: - 20 vehicles.
- High: - 50 vehicles.

3) The environment:
- City Environment.
- Highway Environment.

The metrics collected in the simulation are Packet Loss Rate which is shown in (1)

$$Packet\ Loss\ Rate = 100 - (a / b * 100) \quad (1)$$

Where ‘a’ is the *Received Packets* and ‘b’ is the *Total Packet Sent*.
And the round-trip time is calculated as shown in (2)

$$Round\ Trip\ Time = a + b. \quad (2)$$

Where 'a' is *Time taken from source to destination* and 'b' is *Time taken from destination to source*. These metrics will help to identify and compare between the AODV and GPSR routing protocols.

III. SIMULATION RESULTS

A. *Packet Loss rate*

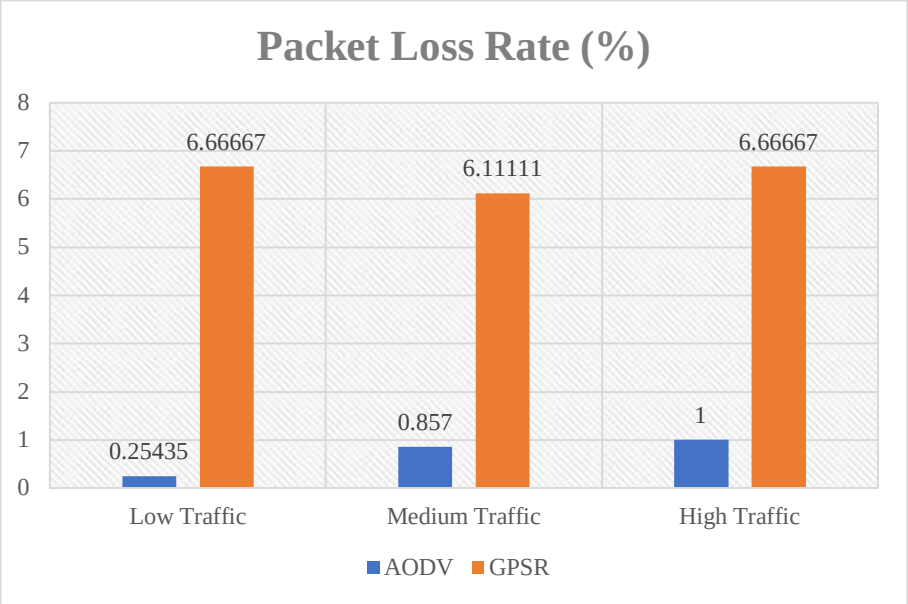


Fig.3. City Scenario Packet Loss Rate

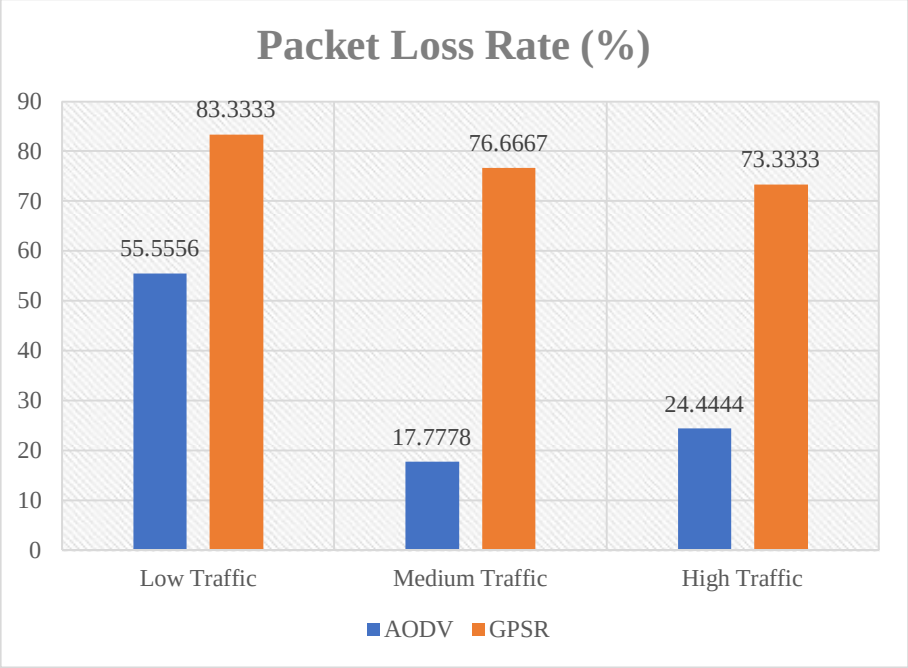


Fig.4. Highway Scenario Packet Loss Rate

Figure 1 and Figure 2 shows the packet loss rate for city and highway scenario in which AODV performs well in both the scenarios. In city scenario, in AODV as the vehicle count increases so does the packet loss rate increases whereas in GPSR the packet loss rate is the same throughout all the vehicle densities.
However, in Highway scenario AODV and GPSR packet loss ratio decreases as the number of vehicles increases.

B. Round Trip Time

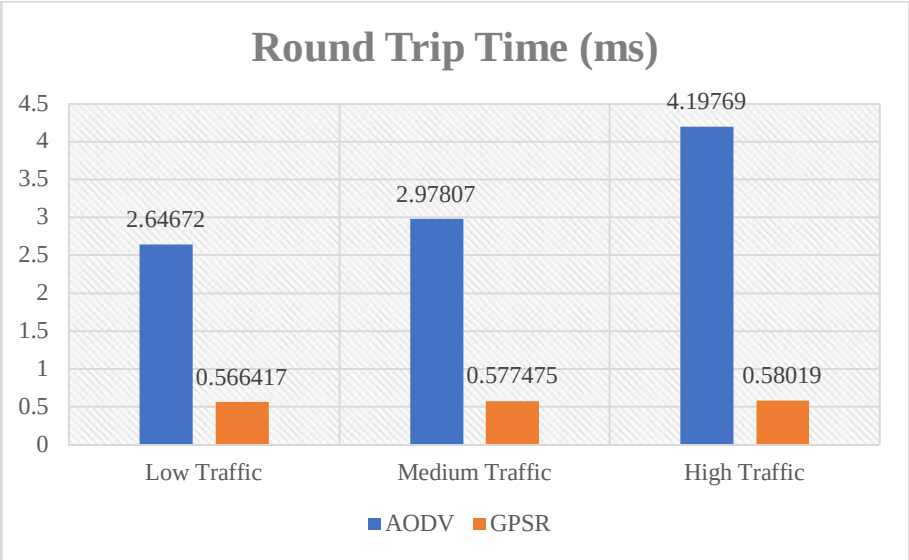


Fig.5. City Scenario Round Trip Time

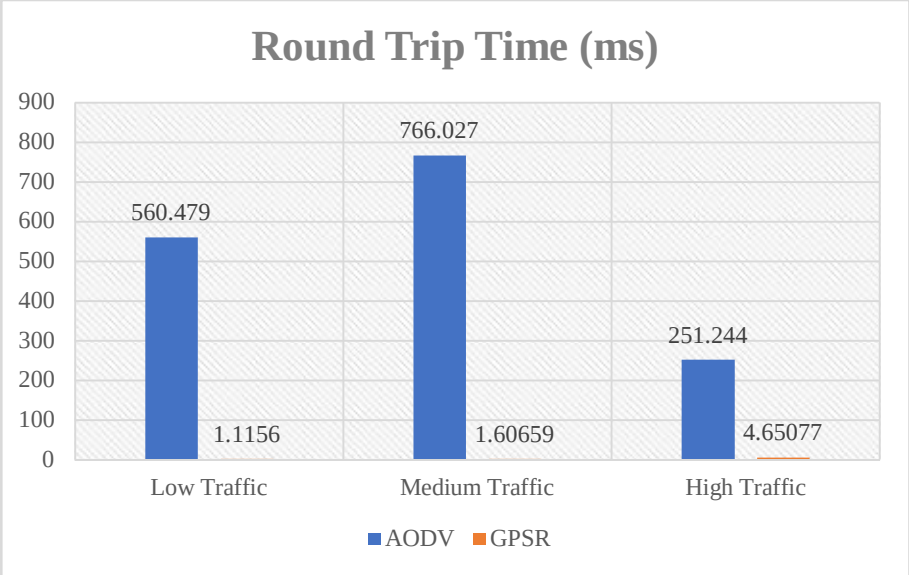


Fig.6. Highway Scenario Round Trip Time

Figure 3 and Figure 4 shows the round-trip time for city and highway scenario in which GPSR performs way better than AODV in both the scenarios. In city scenario AODV round trip time keeps on rising as the number of vehicles increase but the round-trip time of GPSR stays the same as the number of vehicles increase. In highway scenario the round-trip time for AODV decreases as the number of vehicles increases. But GPSR round trip time stays the same with different number of vehicles in highway scenario.

IV. CONCLUSION

In terms of packet loss rate, AODV outperforms GPSR. However, the GPSR round trip time is substantially faster than the AODV. When it comes to applications that do not require a quick response time, such as transmitting telemetry data such as speed, acceleration, weather, infotainment services, and so on, AODV is superior. When it comes to applications that demand a faster response time, such as sending out an alarm after an accident, nearby collision warning systems, etc., GPSR is superior. Hence both of the routing protocols can be used alternatively in different scenarios which requires a node and the RSU units running on 2 wireless interfaces, one running on AODV and the other on GPSR.

V. FUTURE ENHANCEMENTS

Aside from the benefits of VANET adoption, there are a number of hurdles that VANET must overcome. These difficulties might be seen as a future study path or as open research concerns that still require improvement and answers. Some of the challenges that users can take on are as follows:

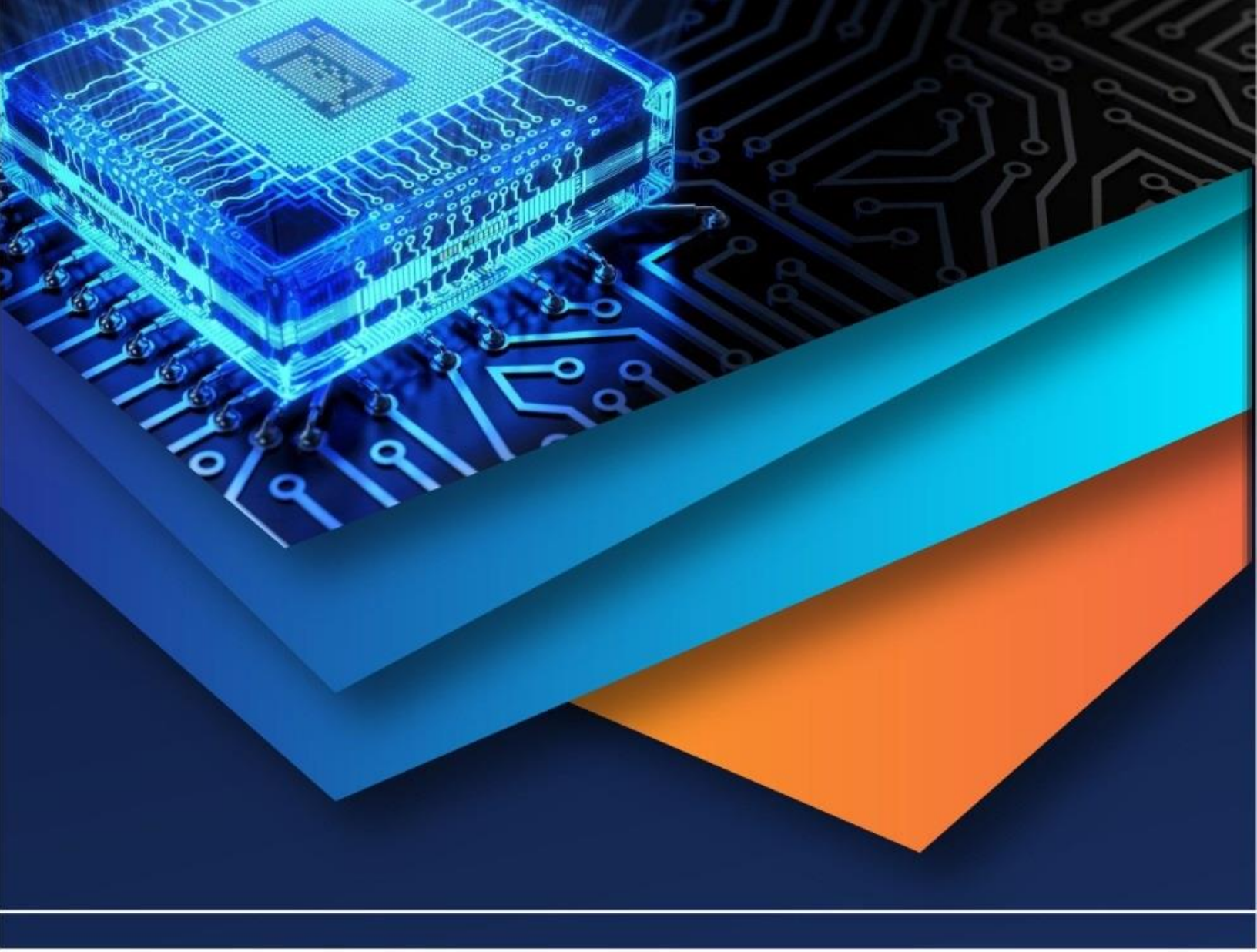
1) *Mobility:* Ad-hoc networks are made up of mobile devices, PDAs, laptops, and other devices as nodes that have restricted mobility or a less mobile nature, whereas nodes in VANET have a very high mobility component. Vehicles make and break touch in a matter of seconds due to the fact that speed is measured in miles per hour. Exchanging information in such a short period of time and with such heterogeneous nodes is an open research issue that necessitates the development of a more advanced and richer network topology model that differs from traditional models that require a higher level of interaction between sender and receiver.
2) *Data Administration and Storage:* Any number of vehicles and other mobile as well as stationary devices can participate in a VANET. For large scale VANET's, number of nodes participating in a VANET can increase up to millions which will in turn generate a large amount of data. Monitoring, managing and storing such a large amount of data is still a challenge which researchers face. Technologies such as Big Data have scope to solve such problem but still merging of two concepts is a research topic.
3) *Quality Service Delivery:* VANET is an open network that allows any node to connect to it. There is no specific system in place to assure the trustworthiness of the nodes. As a result, security becomes a big worry for researchers since communication between nodes occurs through a wireless connection in which any node might transport malicious material and inflict considerable harm to other nodes. Furthermore, identifying such a vehicle is challenging, necessitating the development of more strong security models to assure VANET security. Furthermore, by looking into the VANET, untrustworthy nodes can identify the behaviors, habits, and patterns of other users, posing a major danger to the individual's privacy.
4) *Routing Protocols:* Traditional routing techniques are inappropriate for a VANET because the nodes in a VANET are extremely mobile and can modify the network topology in a couple of seconds. Furthermore, connecting nodes, sharing information between source and destination nodes, and propagating information to additional nodes necessitates the development of resilient algorithms and routing protocols in order to give faster throughput, better service, and an improved packet delivery ratio.

VI. ACKNOWLEDGEMENT

First and foremost, I thank God for granting me the patience, letting me live to see this project through and availing positive people who support me in my entire journey. With profound sense of gratitude and regards, I acknowledge with great pleasure the guidance and support extended by, I thank Dr. Eshwaran Iyer, Dean, Jain Knowledge Campus, Bangalore, Dr. Dinesh Nilkant, Director & Center Head, Jain Knowledge Campus, Bangalore, Dr. M. N. Nachappa, Head, School of CS & IT, Jain (Deemed-to-Be University), Bangalore, Dr. Suchithra R., HoD – M.Sc. I.T., School of CS & IT, Jain (Deem-To-Be University), Bangalore for their interest & encouragement throughout the project. I am very fortunate and grateful to my advisor Dr. M. N. Nachappa, for his valuable comments, continuous support, commitment, encouragement, and suggestions which enabled me pass difficulties with courage and finalize the project work. I don't know where I would be now without huge help in editing my many mistakes. You are truly an outstanding person and an able educator and, I thank you from the bottom of my heart. I am forever thankful to my parents. All your support, encouragements and treatment through helped me a lot.

REFERENCES

[1] M. Musuvathi , "Description of the AODV Protocol," Description of the AODV Protocol, Oct. 08, 2002. https://www.usenix.org/legacy/publications/library/proceedings/osdi02/tech/full_papers/musuvathi/musuvathi_html/node12.html (accessed Aug. 23, 2021).
[2] B. Karp, "Greedy Perimeter Stateless Routing (GPSR)," Greedy Perimeter Stateless Routing (GPSR), Aug. 0, 2000. https://www.icir.org/bkarp/gpsr/gpsr.html#:~:text=Greedy%20Perimeter%20Stateless%20Routing%2C%20GPSR,protocol%20for%20mobile%2C%20wireless%20networks.&text=GPSR%20uses%20greedy%20forwarding%20to,progressively%20closer%20to%20the%20destination. (accessed Apr. 02, 2022).
[3] D. Yuen, "The Future Begins with The Road Side Unit | by Desmond Yuen | Predict | Medium," Medium, Jan. 17, 2022. https://medium.com/predict/edge-computing-is-so-much-more-fun-ac2a8a23e696 (accessed Jan. 24, 2022).
[4] S. Malik and P. K. Sahu, "A comparative study on routing protocols for VANETs - ScienceDirect," A comparative study on routing protocols for VANETs - ScienceDirect, Aug. 30, 2019. https://www.sciencedirect.com/science/article/pii/S2405844019360001 (accessed Sep. 28, 2021).
[5] "MANET Routing Protocols — INET 4.3.0 documentation," MANET Routing Protocols — INET 4.3.0 documentation. https://inet.omnetpp.org/docs/showcases/routing/manet/doc/index.html (accessed Sep. 25, 2021).



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY