FMDB *Transactions on Sustainable Computing Systems*

A Comparative Analysis of Routing Protocols for Efficient Data Transmission in Vehicular Ad Hoc Networks (VANETs)

S. Sajini[1,*], Latha Thamma Reddi[2], R. Regin[3], S. Suman Rajest[4]

[1]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, Tamil Nadu, India.
[2]Department of Automation and Innovation, DXC Technology, Virginia, United States of America.
[3]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Chennai, Tamil Nadu, India.
[4]Department of Research and Development (R&D) & International Student Affairs (ISA), Dhaanish Ahmed College of Engineering, Chennai, Tamil Nadu, India.
sajinis@srmist.edu.in[1], Lata.kodali@dxc.com[2], reginr@srmist.edu.in[3], dean.rnd.tric@dhaanishcollege.co.in[4]

Abstract: Vehicular Ad Hoc Networks (VANETs) are critical in facilitating smart transportation systems, enhancing road safety, and establishing real-time communication between vehicles and infrastructure. The effectiveness of VANETs heavily relies on efficient data transmission, which supports crucial applications like traffic management, collision prevention, and infotainment services. A vital determinant of data transmission efficiency is the routing protocol selection. This research encompasses an extensive comparative analysis of prominent routing protocols used in VANETs to evaluate their capabilities in achieving efficient data transmission. Our findings unveil the strengths and weaknesses of each routing protocol concerning efficient data transmission within the context of VANETs. We pinpoint scenarios where certain protocols excel and highlight challenges some may face. This comparative analysis is a valuable resource for VANET designers, network administrators, and researchers, providing them with the information needed to make well-informed decisions when selecting routing protocols that align with the specific requirements of their VANET applications. Overall, this study significantly contributes to advancing Vehicular Ad Hoc Networks by shedding light on the performance characteristics of routing protocols, specifically optimizing data transmission efficiency. The results presented in this paper aim to promote the development of more robust and dependable VANET systems, ultimately contributing to safer and more efficient vehicular communication on our roadways. Vehicle Ad Hoc Networks (VANETs) are a specialized subset of Mobile Ad hoc Networks where each mobile entity is designated a node. In VANETs, vehicles act as these nodes, enabling data transmission for inter-vehicle communication.

Keywords: Vehicular Ad Hoc Network (VANET); Collision Avoidance; Routing; Road Side Units (RSU); Vehicle to Vehicle Communication (V2V); Security; Infrastructure; Network Security.

Received on: 13/10/2022, **Revised on:** 27/11/2022, **Accepted on:** 05/01/2023, **Published on:** 11/02/2023

Cited by: S. Sajini, L. T. Reddi, R. Regin, S. S. Rajest, “A Comparative Analysis of Routing Protocols for Efficient Data Transmission in Vehicular Ad Hoc Networks (VANETs),” *FMDB Transactions on Sustainable Computing Systems*., vol. 1, no. 1, pp. 1–10, 2023.

1. Introduction

In recent years, technology for vehicular ad hoc networks [1] (VANETs) has evolved. VANET was coined to describe networks that spontaneously form and quickly evolve due to their extremely dynamic character. VANETs, or vehicular ad hoc networks, are adaptable systems designed to connect vehicles for a specific purpose. VANETs are now well-established as trustworthy networks for inter-vehicle communication on highways and in urban contexts. In the event of an emergency, VANETs must

[*] Corresponding author.

communicate with one another despite not being part of the infrastructure. VANETs face the added challenge of underloading due to a lack of infrastructure. Each vehicle in a VANET functions as a node and is responsible for managing and controlling the network's communication. Based on the local wireless networking technology, VANETs are mostly utilised as Vehicle communication (V2V) and Vehicle-to-units (RSU), also known as Vehicle Infrastructure (V2I). This paper's main contribution is a discussion of a comprehensive literature review of VANET difficulties, including those related to communication, threats, VANET assaults, and solutions. Because of their importance to system dependability and user acceptance, security and privacy concerns in VANETs are also discussed here. In conclusion, this article reviews the current VANETs landscape and the remaining VANETs challenges.

When talking about mobile ad hoc networks (MANET), VANET is another type [2]. Due to their network characteristics, the nodes in a MANET are able to communicate with one another even in the absence of a centralised network. However, VANETs have recently come to light as a particularly difficult and risky subset of MANETs. By enabling vehicles to exchange data with one another, VANET improves traffic flow in cities and on highways by revealing road conditions, reducing accidents, and identifying crises.

Vehicular Ad Hoc Networks (VANETs) have emerged as a promising technology that can enhance road safety, traffic management, and passenger comfort by facilitating communication between vehicles and roadside infrastructure. These networks create a dynamic environment where efficient and dependable data transmission protocols are essential. A crucial aspect within VANETs is the selection of an appropriate routing protocol capable of efficiently handling the distinctive challenges posed by rapidly changing network topologies and the high mobility of vehicles. Routing protocols are pivotal in dictating how data packets are directed from their source to their destination within a network. In the context of VANETs, these protocols must address specific difficulties, including frequent shifts in network structure, intermittent connectivity, the rapid movement of nodes, and the imperative for low latency. Consequently, researchers and engineers have devised a range of routing protocols designed specifically for the VANET context, each with its strengths and limitations.

This study presents a comprehensive and thorough comparative analysis of diverse routing protocols tailored to efficiently transmit data within VANETs. The central goal is to assess the performance of these protocols across varied scenarios and conditions, aiming to uncover their advantages and limitations. Network designers can make well-informed choices when selecting a suitable routing protocol for particular VANET applications by comprehending the trade-offs inherent in different routing strategies.

In summary, this paper aims to augment the existing knowledge of VANETs by delivering an intricate comparative analysis of routing protocols. By evaluating their performance across various scenarios, this study seeks to guide network designers, researchers, and practitioners in making well-considered decisions when choosing routing protocols that align effectively with the distinct requisites of vehicular ad hoc networks.

2. Architecture

The purpose of VANET [3] is to facilitate communication between vehicles that are located in close proximity to one another. There are three different domains that make up the VANET.

- Mobile domain: There are two key components to the Mobile space. The first section consists of the many vehicles currently in motion. The second category is the portable gadget, which includes things like smartphones, GPS units, and personal digital assistants.
- Infrastructure domain: Even the infrastructure field can be broken down into two sections. In the first section, we have what we call "Roadside units," which include things like street signs, utility poles, and traffic signals. The second component is the nerve centre, which consists of administrative hubs like the fleet management hub.
- Generic domain: Both public and private networks contribute to the generic domain. A VANET is comprised of several computing devices, including nodes, servers, and others.

The mobile domain and the infrastructure domain both have access to the data shown in Figure 1. Information and communications from the infrastructure domain are then passed on to a generic domain. Users are able to make better use of fixed and mobile resources thanks to the sharing of information between them [4].

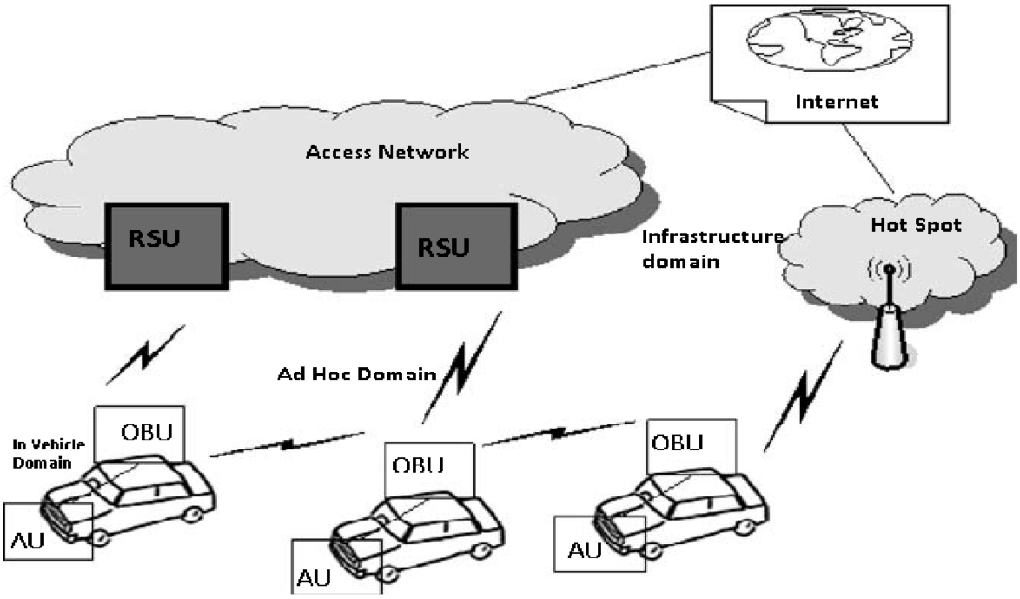

Figure 1: VANET Architecture [4]

Similar to the VANET [5] architecture is another In Figure 2, we see a communication architecture where the various forms of communication are divided into four distinct categories. That would be:

- In-vehicle communication: The vehicle's performance can be maintained, for example, by relaying information about the driver's fatigue, drowsiness, etc. from the vehicle's internal systems. This contributes to the well-being of drivers and pedestrians.
- Vehicle-to-vehicle communication (V2V): The drivers of both vehicles benefit from this exchange of information about the road and any potential hazards they may encounter. V2V operates independently of a network's permanent facilities.
- Vehicle-to-road infrastructure (V2I) communication: The sharing of information between the car and the base units. Sensing the surrounding area and receiving timely traffic and weather reports are both aided by this line of communication.
- When cars talk to the 3G/4G internet, this is called vehicle-to-broadband cloud (V2B) connectivity. The primary function of this is vehicle tracking.

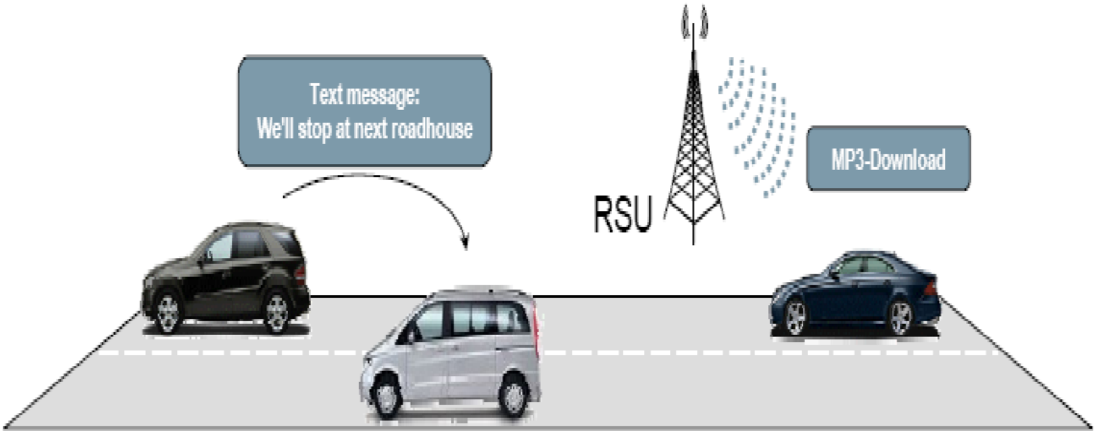

Figure 2: Vehicle to Vehicle Communication

3. Applications of VANET

VANETs [6] are used in the real world for a variety of helpful purposes. The following are examples of applications:

- Safety Oriented Applications: These applications are developed to increase road safety, save lives due to road accidents and also help to increase traffic efficiency. This application is again classified into 3 types.
  - Collision avoidance: This type of application is used at the time of accidents and helps to inform the other vehicles via multi-hop so the other vehicles stay away from that area. Also, this application's messages are in the form of speed, direction, route, etc.
  - Cooperative driving: The application informs about the driving road conditions, such as deep bends, sharp turns, and speed limits. This helps to optimize the journey of the vehicles.
  - Traffic optimization: It’s a data-gathering application. This helps to inform the other drivers about the congestion and critical situations of driving at the place or roads.
- Infotainment applications: Messages from these apps provide drivers and other users with useful information, such as the location of the nearest coffee shop, parking lot, car repair shop, and more.

3.1. Characteristics of VANET

VANET [7-8] is a subcategory of MANET with its distinct characteristics listed as follows.

- High Mobility: Due to the increased mobility of nodes in VANETS, it is more difficult to determine where each node is at any given time, protecting the privacy of each node in the network [9].
- Unpredictable Network topology: No physical support is needed for VANETs. Due to the great mobility, there is frequent movement of the nodes.
- Unbounded network size: The VANETs operate across national borders and throughout multiple cities.
- Adequate information sharing: Due to the necessity of exchanging data between RSUs and vehicles, as well as between vehicles themselves, frequent and excessive node-to-node communication is established.
- Wireless Communication: VANETs are ideally suited to use in mobile, wireless settings. They all talk to one another wirelessly and share information.
- Time Critical: Information exchanged between nodes must occur in a very brief window for it to be successfully delivered.
- Sufficient Energy: Vehicles and RSUs typically have access to ample energy and built-in battery resources, making it possible to carry out labor-intensive procedures. Cryptographic algorithms like RSA, ECDSA, etc.
- Physical Protection: In the wild, VANETs are safer than MANETs. The security of individual nodes in a VANET is thereby increased.

3.2. Security requirements in VANET

We should think about the security needs for a safe and attack-free sharing environment before adopting VANET [10]. The following security precautions are both general and unique to VANET [11]. That would be:

- Authentication: VANET's primary need. This verifies the identity of the person sending the message or making the request. If this condition is not met, severe assaults will be launched. Nodes in a network or in communication with one another can only be trusted if they exhibit one of three characteristics. Identity verification, property verification, and geographical verification are the three main types.
- Integrity: This is also a crucial need for the VANET system. This safeguards against message forgery, modification, or unauthorised data generation, and guarantees delivery to the authenticated user.
- Confidentiality: In order to prevent unauthorised parties from gaining access to private information shared between nodes or RSU, the transmitted message must be encrypted.
- Availability: Critical conditions, such as attacks or failures, should not disrupt the network or the application. The system must be able to recover from errors.
- Access control: The network's other nodes should not overhear conversations between the police and the ambulance service, for example, in which responsibilities and privileges are being determined.
- Unlink ability: Connecting one node to another is characterised by this as well. A path is established in a VANET, and this path consists of the set of nodes between the origin and the destination. This feature guarantees that all nodes in the network will recognise the communication between the source and the target.

3.3. Attackers on Vehicular Network

Protecting a network requires an understanding of the various attacks that might bring it down. Attackers in VANET [12-13] can be broken down into three distinct types.

- Insider and Outsider: Attackers from within are those who have access to the network and have been given credentials. The invaders are the assailants from the outside.
- Malicious and Rational: While logical attacks gain from attacks and are predictable, malicious ones are always doing more harm than good to the network's functionality. During a conversation, rational attackers may steal, alter, or replace data.
- Active and Passive: Attackers can be classified as either active or passive, with the former generating signals and packets and the latter only sensing activity in the network.

3.4. Attacks in the VANET

It is important to understand the many forms of network assault, when they occur, and by what kind of attackers [14-15] in order to construct a network free of attackers and to ensure safe communication.

- Impersonate: In an impersonate attack, the attacker poses as a trusted node in order to get access to its resources.
- Session hijacking: The majority of authentication is completed at session startup. The session between the nodes is compromised in this attack.
- Identity revealing: A driver is often the car's owner. Therefore, obtaining the owner's identify may compromise confidentiality.
- Repudiation: Repudiation is most dangerous when a communicating node denies or attempts to deny the message.
- Eavesdropping: This is the most typical form of information disclosure. The target of this attack is sensitive information.
- Denial of Service: In this type of attack, the malicious user is denied access to the service via the victim node.
- Privacy and Security Options for VANETs

Considering the attacks listed above, we must deploy secured and authenticated VANETs. Focusing on all the aspects of attacks creating this kind of setting takes a lot of time and effort. Examining and analysing the concept of routing is crucial for creating and deploying a vulnerable, secure, and legitimate VANET.

5. Routing

The VANETs would not function without routing. A network cannot be formed in an infrastructure-free setting without routing [16, 17]. Choosing an encrypted and verified path takes time and effort. Here, routing is crucial because it facilitates the exchange of keys and the transmission of messages. Connecting trusted nodes along a path facilitates secure key exchange and encrypted data transmission. Figure 3 displays the full range of available routing protocols. In addition to security, other elements such as routing supporting environment, forwarding strategy, Predictive, Buffering, Overlay and non-overlay, and positioning system should be considered while choosing a routing protocol for VANETs. Below is a list of some of the recommendations that were made in response to the call for such routes.

Through simulation-based tests, the researchers contrasted the performance of four well-known routing protocols in VANETs: AODV, DSDV, DSR, and OLSR. Their findings underscored the substantial impact of the selected routing protocol on network efficiency, particularly on factors such as network density and the velocity of vehicles [18]. The analysis was broadened to encompass more recent protocols like V-ADD and GPCR, in addition to conventional ones.

The investigation was centred on scenarios set in urban and highway environments, taking into account variables such as network density and the mobility of nodes. The outcomes unveiled the respective advantages and drawbacks of each protocol within distinct scenarios [19]. Investigated the influence of vehicle concentration and traffic circumstances on the effectiveness of AODV, OLSR, and DSR routing protocols.

The analysis illuminated that these protocols displayed divergent performance outcomes contingent on the network density and the traffic volume [20]. investigated the efficiency of VANET routing protocols in urban grid layouts. The study compared DSDV, AODV, and OLSR and observed that protocol performance was influenced by factors like intersection density and vehicle speed [21]. Examined the effectiveness of VANET routing protocols within urban grid configurations.

The research involved a comparison between DSDV, AODV, and OLSR, highlighting that the performance of these protocols was susceptible to factors such as the density of intersections and the speed of vehicles [22]. Conducted experiments to compare the performance of several protocols, including AODV, AOMDV, DSR, and DSDV, in scenarios with different traffic densities and road layouts. The authors found that each protocol excelled under specific conditions [23].

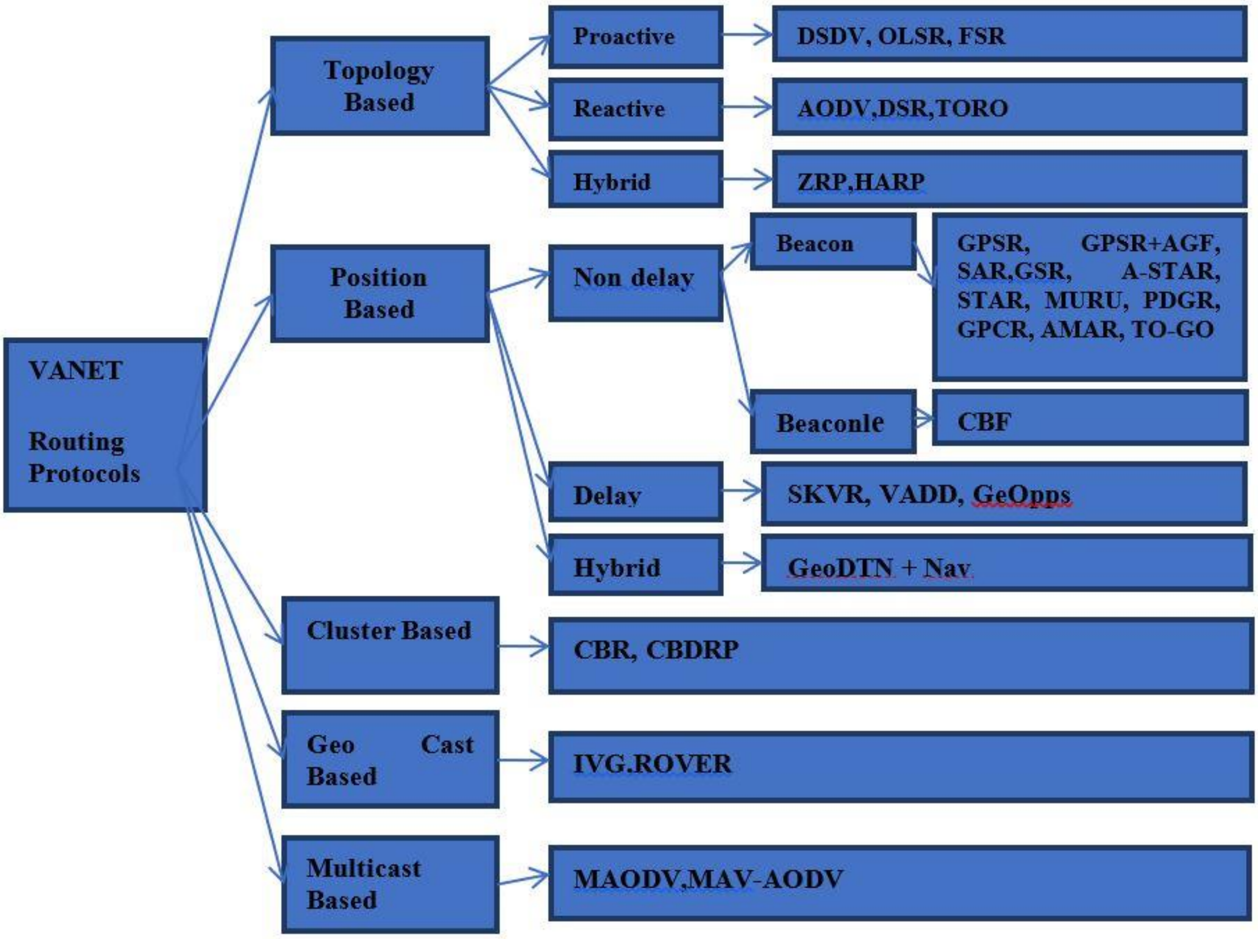

Figure 3: VANET routing protocol

The present body of related research demonstrates a variety of comparative assessments of routing protocols for VANETs [24-27]. These investigations have offered valuable understandings of how different protocols perform across a spectrum of scenarios, aiding researchers and professionals in making knowledgeable choices regarding selecting routing approaches for particular VANET uses [28].

Future studies could explore more sophisticated routing protocols and examine emerging technologies that might influence VANETs [29-31].

6. Comparison of VANET Routing Protocols

Several scholars have carried out comparative investigations to assess the effectiveness of routing protocols for Vehicular Ad Hoc Networks (VANETs) across various situations [32]. These examinations commonly utilize simulation-based experiments to quantify a range of metrics, encompassing factors like the ratio of successfully delivered packets, the delay experienced from source to destination [47], the capacity for data transfer, and the overhead associated with routing processes (table 1) [33-37].

Table 1: Comparison and Issues Related to Secure Authentication Protocol For VANETS

VANET Protocol	Environment	Forwarding Strategy	Predictive	Buffering carry and forwarding strategy	Overlay or Non-overlay	Positioning System required
DSDV, GSRP, FSR OLSR, WRP, TBRPF, ZRP, HARP	Urban	Multi-hop	No	No	No	No
TORA, AODV, DSR, AODV+PGB	Urban	Multi-hop	No	Yes	No	No
PRAODV	Urban	Multi-hop	Yes	Yes	No	No
GPSR	Urban	Greedy	No	No	No	Yes
GPSR+AGF	Highway	Greedy	No	No	No	Yes
GSR	Urban	Greedy	No	No	Yes	Yes
SAR	Urban	Greedy	No	No	No	Yes
A-TAR, STAR	Urban	Greedy	No	No	Yes	Yes
MURU	Urban	Greedy	Yes	No	No	Yes
GPCR	Urban	Greedy	No	No	Yes	Yes
GpsrJ+	Urban	Greedy	Yes	No	Yes	Yes
GPGR	Urban	Greedy	Yes	No	No	Yes
PBRDV	Urban	Greedy	No	No	No	Yes
CAR	Urban	Greedy	No	No	Yes	Yes
GyTAR, JARR, LOUVRE	Urban	Greedy	Yes	No	Yes	Yes
DIR, ROMSGP, AM, AR, EBGR, B-MFR	Urban	Greedy	No	No	No	Yes
TO-GO	Urban	Greedy	Yes	No	No	Yes
SKVR	Urban	Greedy	No	Yes	No	No
VADD	Urban	Greedy	No	Yes	No	No
GeOpps, GeoDTN+Nav, LOR A-CBF	Urban		No	Yes	No	No
CBR, CBDRP, COIN, TIBCRPH	Urban	Multi-hop	No	Yes	No	Yes
IVG	Highway	Multi-hop	No	No	No	Yes
CGR, AGR, ROVER, Mobicast	Urban	Multi-hop	No	No	No	Yes

MAODV, ADMR, MOLSR, ODMRP, D- ODMRP	Urban	Multi-hop	No	No	No	No

VANETs are a safe, authentic, and collision-free way to communicate. The core ideas revolved around the transfer of data securely using different routing techniques [38-42]. Security, integrity, non-repudiation, forward and backward secrecy, unlikeability, anonymity, conspiracy, and more over energy efficiency and usage, less storage are all factors to consider while designing a safe and effective authentication system. After taking all of the factors into account, designing a fool proof authentication system for vanes is a time-consuming process. Because we prioritise safety by means of a routing mechanism, we eliminate data transmission delays. There are many difficulties in VANET [43-45]. There will be insufficient resources for storing energy and colliding. In terms of routing security, AODV is one of the safest options available. High traffic in a network can be avoided if we take the cost of authenticating each node and each message into account [46]. The choice of a sophisticated authentication technique, which in turn is dependent on the chosen key-sharing scheme, is also important.

7. Conclusion

The thorough analysis of routing protocols for effective data transmission in Vehicular Ad Hoc Networks (VANETs) has yielded valuable insights into the performance characteristics of diverse routing protocols within this dynamic and challenging environment. The primary objective of this study was to address the critical necessity for optimized data transmission in VANETs, specifically to support critical applications like traffic management, collision avoidance, and real-time vehicle-to-vehicle communication. We meticulously evaluated how each protocol performed under varied traffic conditions, network densities, and mobility patterns by combining simulated experiments and real-world scenarios. The outcomes unveiled that different routing protocols exhibit excellence in specific scenarios while facing challenges in others. These insights represent a valuable resource for VANET designers, network administrators, and researchers, providing them with the knowledge necessary to make informed decisions when selecting routing protocols that align with the unique demands of their VANET applications. A key lesson from this study underscores the vital importance of context. The performance of a routing protocol can exhibit significant variation based on the specific attributes of the VANET, such as network size, vehicle density, mobility patterns, and the presence of infrastructure. Therefore, a thorough comprehension of the operational context is essential to achieve the utmost data transmission efficiency in VANETs

In conclusion, this research substantially contributes to advancing Vehicular Ad Hoc Networks by comprehensively comparing routing protocols. By grasping the strengths and limitations of these protocols, we can make strides toward creating more robust and dependable VANET systems, thereby enhancing safety and efficiency in vehicular communication on our roadways. Future endeavours in this field should persist in exploring evolving routing protocols while considering supplementary factors, such as security and scalability, to further amplify the performance of VANETs.

Acknowledgement: The support of all my co-authors is highly appreciated.

Data Availability Statement: This study uses online benchmark data to conduct the research. This is a fresh study done by the authors.

Funding Statement: No funding has been obtained to help prepare this manuscript and research work.

Conflicts of Interest Statement: No conflicts of interest have been declared by the author(s). This is the authors' fresh work. Citations and references are mentioned as per the used information.

Ethics and Consent Statement: The consent has been obtained from the colleges during data collection and has received ethical approval and participant consent.

References

1. H. Hartenstein and L. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," in IEEE Communications Magazine, vol. 46, no. 6, pp. 164-171, June 2008.
2. M. A. Sabih Ur Rehman and T. A. Khan, "Lihong Zheng, Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges," Journal of Wireless Networking and Communications, vol. 3, no. 3, pp. 29–38, 2013.
3. R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Comput. Commun., vol. 44, pp. 1–13, 2014.

4. R. Shringar Raw, M. Kumar, and N. Singh, “Security Challenges, Issues and Their Solutions For Vanet,” Int. J. Netw. Secur. Appl., vol. 5, no. 5, pp. 95–105, 2013.
5. F. Cunha et al., “Data communication in VANETs: Protocols, applications and challenges,” Ad Hoc Netw., vol. 44, pp. 90–103, 2016.
6. R. Brendha and V. S. J. Prakash, "A survey on routing protocols for vehicular Ad Hoc networks," 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, pp. 1-7, 2017.
7. K. N. Qureshi, A. H. Abdullah, J. Lloret, and A. Altameem, “Road-aware routing strategies for vehicular ad hoc networks: Characteristics and comparisons,” Int. J. Distrib. Sens. Netw., vol. 12, no. 3, p. 1605734, 2016.
8. Z. Lu, G. Qu, and Z. Liu, “A survey on recent advances in vehicular network security, trust, and privacy,” IEEE Trans. Intell. Transp. Syst., vol. 20, no. 2, pp. 760–776, 2019.
9. F. Qu, Z. Wu, F. -Y. Wang and W. Cho, "A Security and Privacy Review of VANETs," in IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 6, pp. 2985-2996, Dec. 2015, doi: 10.1109/TITS.2015.2439292.
10. J. Bernsen and D. Manivannan, “Unicast routing protocols for vehicular ad hoc networks: A critical comparison and classification,” Pervasive Mob. Comput., vol. 5, no. 1, pp. 1–18, 2009.
11. T. Sawamura, K. Tanaka, M. Atajanov, N. Matsumoto, and N. Yoshida, “Adaptive router promotion and group forming in ad-hoc networks,” Int. J. Ad Hoc Ubiquitous Comput., vol. 3, no. 4, p. 217, 2008.
12. H. Menouar, F. Filali, and M. Lenardi, “A survey and qualitative analysis of mac protocols for vehicular ad hoc networks,” IEEE Wirel. Commun., vol. 13, no. 5, pp. 30–35, 2006.
13. T. W. Chim, S. M. Yiu, L. C. K. Hui and V. O. K. Li, "Security and Privacy Issues for Inter-vehicle Communications in VANETs," 2009 6th IEEE Annual Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops, Rome, Italy, pp. 1-3,2009.
14. B. Parno and A. Perrig, “Challenges in securing vehicular networks,” in Proceedings of the Workshop on Hot Topics in Networks, HotNets-IV; College Park, MD, USA, pp. 1–6, 2005.
15. A. Rawat, S. Sharma, and R. Sushil, “VANET: Security attacks and its possible solutions,” J. Inf. Oper. Manag, vol. 3, pp. 301–304, 2012.
16. X. Lin, X. Sun, P.-H. Ho, and X. Shen, “GSIS: A secure and privacy-preserving protocol for vehicular communications,” IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3442–3456, 2007.
17. P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, “Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks,” IEEE Trans. Intell. Transp. Syst., vol. 17, no. 4, pp. 1015–1028, 2016.
18. R. Kalkundri and S. A. Kulkarni, “A Secure Message Authentication Scheme for VANET using ECDSA,” in Proceeding 4th International Conference on Computing Communications Networking Technologies (ICCCNT), Tiruchengode, India, pp. 1–6, 2013.
19. N. B. Bhavesh, S. Maity, and R. C. Hansdah, “A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs,” in 2013 27th International Conference on Advanced Information Networking and Applications Workshops, 2013.
20. F. Qu, Z. Wu, F. Wang, and W. Cho, “A security and privacy review of VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 16, no. 6, pp. 2985–2996, 2015.
21. C. Zhang, R. Lu, X. Lin, and P. H. Ho, “ShenAn efficient identity based batch verification scheme for vehicular sensor networks,” in Proc. IEEE International Conference on Computer Communications, pp. 816–824, 2008.
22. J. Li, H. Lu and M. Guizani, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 4, pp. 938-948, April 2015, doi: 10.1109/TPDS.2014.2308215.
23. A. Smitha, M.M.P. Manohara, N. Ajam, J. MouznaAn optimized adaptive algorithm for authentication of safety critical messages in VANET Proc. 8th International Conference on Communications and Networking in China, CHINACOM-2013, pp. 149-154, 2013.
24. C. R. Mahesha et al., “Effect of friction stir welding on the mechanical and microstructural behaviour of AA7075 aluminium alloy,” Adv. Mater. Sci. Eng., vol. 2022, pp. 1–8, 2022.
25. D. K. Sharma, B. Singh, M. Raja, R. Regin, and S. S. Rajest, “An Efficient Python Approach for Simulation of Poisson Distribution,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
26. D. K. Sharma, B. Singh, R. Regin, R. Steffi, and M. K. Chakravarthi, “Efficient Classification for Neural Machines Interpretations based on Mathematical models,” in 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), 2021.
27. D. K. Sharma, N. A. Jalil, R. Regin, S. S. Rajest, R. K. Tummala, and Thangadurai, “Predicting network congestion with machine learning,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021

28. D. Uike, S. Agarwalla, V. Bansal, M. K. Chakravarthi, R. Singh and P. Singh, "Investigating the Role of Block Chain to Secure Identity in IoT for Industrial Automation," 2022 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 837-841,2022.
29. F. Arslan, B. Singh, D. K. Sharma, R. Regin, R. Steffi, and S. Suman Rajest, “Optimization technique approach to resolve food sustainability problems,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
30. G. A. Ogunmola, B. Singh, D. K. Sharma, R. Regin, S. S. Rajest, and N. Singh, “Involvement of distance measure in assessing and resolving efficiency environmental obstacles,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
31. G. Karagiannis et al., “Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions,” IEEE Commun. Surv. Tutor., vol. 13, no. 4, pp. 584–616, 2011.
32. G. P. Reddy, Y. V. P. Kumar, and M. K. Chakravarthi, “Communication technologies for interoperable smart microgrids in urban energy community: A broad review of the state of the art, challenges, and research perspectives,” Sensors (Basel), vol. 22, no. 15, 2022.
33. J. M. Fuentes and A. I. Gonzalez-Tablas, “RibagordaOverview of security issues in vehicular ad hoc networks,” in Handbook of Research on Mobility and Computing, M. M. Cruz-Cunha and F. Moreira, Eds. Pennsylvania: IGI Global, pp. 1–17, 2010.
34. K. Sharma, B. Singh, E. Herman, R. Regine, S. S. Rajest, and V. P. Mishra, “Maximum information measure policies in reinforcement learning with deep energy-based model,” in 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), 2021.
35. M. Bellare, “Rogaway Message authentication M. Bellare, Introduction to Modern Cryptography,” pp. 155–175, 2005.
36. M. N. Mejri, J. Ben-Othman, and M. Hamdi, “Survey on VANET security challenges and possible cryptographic solutions,” Veh. Commun., vol. 1, no. 2, pp. 53–66, 2014.
37. M. S. Sheikh, J. Liang, and W. Wang, “Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey,” Wirel. Commun. Mob. Comput., vol. 2020, pp. 1–25, 2020.
38. P. Reddy, Y. Gogulamudi, and A. Maddikera Kalyan Chakravarthi, “Refined Network Topology for Improved Reliability and Enhanced Dijkstra Algorithm for Optimal Path Selection during Link Failures in Cluster Microgrids,” Sustainability, vol. 14, no. 16, 2022.
39. R. Jain et al., “Internet of Things-based smart vehicles design of bio-inspired algorithms using artificial intelligence charging system,” Nonlinear Eng., vol. 11, no. 1, pp. 582–589, 2022.
40. S. K. Bhoi and P. M. Khilar, “Vehicular communication: a survey,” IET Netw., vol. 3, no. 3, pp. 204–217, 2014.
41. S. Sonnad, M. Sathe, D. K. Basha, V. Bansal, R. Singh and D. P. Singh, "The Integration of Connectivity and System Integrity Approaches using Internet of Things (IoT) for Enhancing Network Security," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, pp. 362-366, 2022.
42. T. Shrikant S and M. Sunilkumar S, “A survey on attacks, security and trust management solutions in VANETs,” in 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), 2013.
43. V. Bansal, S. Pandey, S. K. Shukla, D. Singh, S. A. Rathod and J. L. A. Gonzáles, "A Frame Work of Security Attacks, Issues Classifications and Configuration Strategy for IoT Networks for the Successful Implementation," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1336-1339,2022.
44. V. Gunturu, V. Bansal, M. Sathe, A. Kumar, A. Gehlot and B. Pant, "Wireless Communications Implementation Using Blockchain as Well as Distributed Type of IOT," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, pp. 979-982,2023.
45. V. Suthar, V. Bansal, C. S. Reddy, J. L. A. Gonzáles, D. Singh and D. P. Singh, "Machine Learning Adoption in Blockchain-Based Smart Applications," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, pp. 372-378,2022.
46. Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, “Vehicle Ad Hoc networks: applications and related technical issues,” IEEE Commun. Surv. Tutor., vol. 10, no. 3, pp. 74–88, 2008.
47. B. T. Sharef, R. A. Alsaqour, and M. Ismail, “Vehicular communication ad hoc routing protocols: A survey,” J. Netw. Comput. Appl., vol. 40, pp. 363–396, 2014.