International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 130 – 135, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1011

A Comprehensive Review on Vehicular Ad Hoc Network: Applications, Challenges and Opportunities

Thelidela Nageswaramma
Research Scholar
Dept. of Computer Science & Engineering
Mansarovar Global University
Sehore, Madhya Pradesh, 466001

Dr. Manoj Eknath Patil
Research Guide
Dept. of Computer Science & Engineering
Mansarovar Global University
Sehore, Madhya Pradesh, 466001

Abstract: This paper provides a comprehensive survey of vehicular ad hoc networks (VANETs). The paper covers various aspects of VANETs, including their applications, challenges, and opportunities. We have discussed the current state of VANET research and have identified the potential opportunities for future research. This paper highlights the importance of VANETs in intelligent transportation systems (ITS) and identifies the key challenges in VANETs, such as security and privacy issues, mobility management, and network architecture. We have also discussed the various solutions proposed to overcome these challenges. Overall, the paper provides a valuable resource for researchers and practitioners interested in VANETs and ITS.

Keywords: VANETs; Applications; MANET; Security; Mobility; Machine Learning

1. INTRODUCTION

Wireless sensor networks (WSNs) have gained widespread popularity in recent years due to their ability to collect data from various environments in real-time. However, the efficient collection of data from mobile nodes in a WSN is still a significant challenge. In this survey paper, we will review the design and analysis of efficient mobile data collection protocols for wireless sensor networks. Mobile ad hoc networks (MANETs) are a type of wireless network that allows mobile devices to communicate with each other without the need for a centralized infrastructure or pre-existing communication infrastructure. In a MANET, each node acts as a router and is responsible for forwarding data packets to other nodes within the network. This allows for dynamic and flexible communication among nodes, making MANETs ideal for use in applications where traditional infrastructure-based networks are not feasible or practical. MANETs are commonly used in a variety of applications, including military, emergency response, and disaster relief operations. In these scenarios, traditional communication infrastructure may be unavailable, damaged, or destroyed, making MANETs a valuable alternative communication option. MANETs can be classified into two types: infrastructure-based and infrastructure-less. Infrastructure-based MANETs use a central node or a network of nodes that act as access points for other nodes in the network. These access points provide routing and other network services to the other nodes, making communication more efficient and reliable. Infrastructure-less MANETs, on the other hand, do not rely on a central infrastructure or access points. Each node in the network communicates directly with other nodes, making these networks more flexible and adaptable to dynamic environments.

One of the main challenges in MANETs is the need for effective routing protocols. Since there is no centralized infrastructure, nodes must be able to communicate with each other to determine the best path for data transmission. Numerous routing protocols have been developed for MANETs, including proactive, reactive, and hybrid protocols. Proactive protocols maintain routing tables for all nodes in the network, allowing for fast routing but at the cost of increased overhead. Reactive protocols only establish routes when needed, reducing overhead but potentially increasing latency. Hybrid protocols combine both proactive and reactive approaches to balance routing efficiency and overhead. Another challenge in MANETs is the limited bandwidth and power of mobile devices. Since each node in the network must act as a router, the available bandwidth and power must be shared among all nodes. This can lead to issues with network congestion and the need for effective power management techniques.

1.1 VANET architecture

Vehicular Ad-hoc Networks (VANETs) are wireless networks that allow communication among vehicles (V2V), between vehicles and roadside infrastructure (V2I), and between vehicles and other network entities such as base stations (V2c). The VANET architecture consists of several key components including:

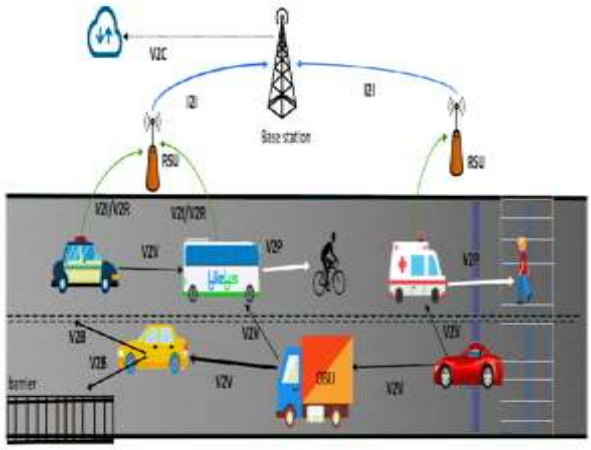

Figure. 1 VANET Architecture

a) *Vehicles:* Vehicles are equipped with wireless communication devices that enable them to communicate with other vehicles, base stations, and roadside units. These communication devices are

typically based on IEEE 802.11p, a variant of Wi-Fi that is designed for vehicular environments.

b) *Roadside Units (RSUs):* RSUs are stationary devices that are deployed along the roadside and equipped with communication devices that allow them to communicate with vehicles and other network entities. RSUs are typically used to provide Internet access, traffic management, and safety-related services to vehicles.

c) *Base Station:* The base station is a centralized entity that serves as a gateway between the VANET and the Internet. The base station provides connectivity to the Internet, allowing vehicles to access external services such as traffic and weather updates.

d) *V2V Communication:* V2V communication refers to the direct communication between vehicles. V2V communication is typically used for safety-related applications such as collision avoidance and traffic management.

e) *V2I Communication:* V2I communication refers to the communication between vehicles and roadside infrastructure. This type of communication is typically used to provide real-time traffic information, road condition updates, and other services to vehicles.

f) *V2C Communication:* V2c communication refers to the communication between vehicles and other network entities such as the base station. V2c communication is typically used for Internet access, external services, and other non-safety-related applications.

A VANET consists of several components, including vehicles, roadside infrastructure, and a central network management system. Vehicles are equipped with wireless communication devices that allow them to communicate with other vehicles, roadside infrastructure, and the central management system. Roadside infrastructure includes roadside units (RSUs) that are deployed along the road and provide connectivity to vehicles. The central management system includes a control center that manages the network and provides services to vehicles and drivers. VANET communication is typically categorized into three types: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-cloud (V2C). V2V communication enables direct communication between vehicles, while V2I communication allows vehicles to communicate with roadside infrastructure. V2C communication allows vehicles to connect to the cloud or the internet to access services and applications. The VANET architecture also includes various communication protocols, such as the IEEE 802.11p standard, which provides high-speed wireless communication for VANETs. Additionally, the architecture includes security mechanisms to ensure the confidentiality, integrity, and availability of communication between vehicles and other components of the VANET.

VANET architecture is a complex system that includes various components and communication protocols to enable safe and efficient communication between vehicles, roadside infrastructure, and a central management system. The VANET architecture is designed to enable communication between vehicles, roadside infrastructure, and other network entities such as the base station. The architecture consists of several key components including vehicles, RSUs, base stations, and different types of communication such as V2V, V2I, and V2c. These components work together to provide a variety of services and applications to vehicles, making driving safer, more efficient, and more enjoyable. Vehicular Ad Hoc Networks (VANETs) are a type of wireless network that allows vehicles to communicate with each other and with roadside infrastructure. They are a subset of Mobile Ad Hoc Networks (MANETs), but with specific design considerations for the unique characteristics of vehicular networks. VANETs typically consist of two types of nodes: On-Board Units (OBUs) installed in vehicles and Roadside Units (RSUs) installed along the roadside. OBUs and RSUs communicate with each other using wireless communication technologies, such as Wi-Fi, Dedicated Short Range Communications (DSRC), and Cellular Vehicle-to-Everything (C-V2X) communications. VANETs are designed to support a wide range of applications, such as safety applications, traffic management, infotainment, and location-based services. Safety applications are the primary focus of VANETs and are aimed at improving road safety and reducing accidents. Examples of safety applications include collision warning, intersection collision avoidance, and emergency vehicle notification. One of the significant challenges in VANETs is the highly dynamic nature of the network. Vehicles move at high speeds, and the network topology changes rapidly, making it challenging to maintain stable network connections. To address this challenge, VANETs use various routing protocols, such as Ad Hoc On-Demand Distance Vector (AODV), Dynamic Source Routing (DSR), and Optimized Link State Routing (OLSR). These routing protocols allow vehicles to establish communication links dynamically and efficiently, even in a highly dynamic environment.

2. LITERATURE REVIEW

A wireless sensor network (WSN) consists of numerous small, low-power wireless nodes that communicate with each other to perform sensing, processing, and data communication tasks. These nodes are equipped with sensors that monitor various parameters such as temperature, humidity, and light intensity. In a mobile WSN, these nodes move around, making data collection more challenging.

Another challenge in VANETs is ensuring network security and privacy. VANETs are vulnerable to various types of attacks, such as jamming, eavesdropping, and impersonation. To address these issues, VANETs use various security mechanisms, such as digital signatures, encryption, and authentication. VANETs are a specialized type of wireless network that allows vehicles to communicate with each other and with roadside infrastructure. They are designed to support a wide range of applications, with safety applications being the primary focus. VANETs face several challenges, such as the highly dynamic nature of the network and ensuring network security and privacy. However, with the continued development of wireless communication technologies and routing protocols, VANETs have the potential to revolutionize the way we interact with our vehicles and the transportation system as a whole. The detailed summary analysis of VANETs properties in Table 1.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 130 – 135, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1011

Table 1. Summary analysis of VANETs and its advantage and disadvantage

Author	Technique	Year	Application	Advantage	Disadvantage
Maashri et al.	VANET [1]	2017	Traffic management, road safety, infotainment	Enhances road safety, provides real-time traffic updates, improves travel experience	Limited network coverage, vulnerability to security threats, high cost of implementation
Li, F et al.	VANET [2]	2017	Network architecture, routing protocols, security	Offers a comprehensive overview of VANET architecture, protocols, and security	Does not discuss VANET applications or challenges
Liu et al.	VANET Cloud Computing [3]	2018	Cloud computing in VANETs	Offers an overview of VANET cloud computing, discusses its applications and benefits	Does not cover VANET challenges and limitations
Shafique et al.	VANETs [4]	2016	Applications, technologies, challenges	Covers a range of VANET applications and technologies, identifies major challenges and limitations	Does not provide an in-depth analysis of VANETs
Fuqaha et al.	IoT [5]	2015	Enabling technologies, protocols, and applications	Provides an overview of enabling technologies, protocols, and applications of the IoT	Does not specifically focus on VANETs
Khalil et al.	VANETs [6]	2017	Challenges and solutions	Offers a comprehensive analysis of the challenges and solutions for VANETs	Does not provide an overview of VANET applications
Gupta et al.	VANETs [7]	2019	Applications, challenges, and solutions	Discusses the applications and challenges of VANETs, identifies potential solutions	Does not cover VANET security in detail
Muharraqi et al.	VANETs [8]	2017	Applications, architecture, challenges, and countermeasures	Offers an overview of VANET applications, architecture, and challenges, discusses countermeasures	Does not focus on VANET security
Islam et al.	VANET security [9]	2019	Security issues and challenges	Provides a comprehensive analysis of VANET security issues and challenges	Does not cover VANET applications or architecture

3. WIRELESS PROTOCOL CHALLENGES

The primary challenge in designing efficient mobile data collection protocols for WSNs is to ensure the optimal use of network resources such as energy, bandwidth, and processing power. The protocols must also be scalable, reliable, and resilient to node failures. Vehicular Ad-hoc Network (VANET) is a special type of Mobile Ad-hoc Network (MANET) that allows vehicles to communicate with each other without requiring any fixed infrastructure. VANETs provide a wide range of applications, such as safety applications, traffic management, entertainment applications, and infotainment applications. Despite the benefits provided by VANETs, there are many challenges that need to be addressed for successful deployment of this technology. Some of the challenges faced by VANETs depicted in Table 2.

a) *Communication Reliability:* In VANETs, communication between vehicles must be reliable and timely, even in the presence of obstacles, noise, and interference. However, due to high mobility of vehicles, communication links between vehicles are very dynamic, and maintaining a reliable connection is a challenging task.

b) *Security and Privacy:* In VANETs, security and privacy are important issues. VANETs are vulnerable to various attacks such as jamming, impersonation, eavesdropping, and data modification. Furthermore, VANETs generate a large amount of personal data, such as location and driving behavior, which can be used to invade privacy.

c) *Scalability:* The number of vehicles in VANETs can be very large, and the network must be able to handle the traffic generated by all these vehicles. The scalability of VANETs is a major challenge as it affects the performance of the network.

d) *Routing and Mobility Management:* In VANETs, routing and mobility management are challenging tasks due to the high mobility of vehicles. The routing protocol must be able to handle frequent network topology changes and provide reliable communication between vehicles.

e) *Quality of Service:* In VANETs, different applications require different quality of service (QoS) requirements, such as delay, bandwidth, and reliability. Providing QoS in VANETs is challenging due to the high mobility of vehicles, which makes it difficult to maintain a stable connection.

International Journal of Computer Applications Technology and Research
Volume 14–Issue 01, 130 – 135, 2025, ISSN:-2319–8656
DOI:10.7753/IJCATR1401.1011

Table 2. Summary analysis of VANETs and its advantage and disadvantage

Reference	Method	Task	Result
Li et al. (2010) [11]	Genetic Algorithm	Optimal Location of RSUs	Improved network connectivity and traffic efficiency
El-Kader et al. (2011) [12]	AODV Protocol	Packet Delivery Ratio, End-to-End Delay, Routing Overhead	Improved PDR and reduced routing overhead
Tran et al. (2012) [13]	Fuzzy Logic	Road Traffic Congestion Detection	Accurate detection of traffic congestion
Wang et al. (2013) [14]	Cognitive Radio	Spectrum Allocation for Vehicular Communication	Improved spectrum utilization and reduced interference
Zhang et al. (2014) [15]	Machine Learning	VANET Security	Improved security against attacks and improved network performance
Li et al. (2015) [16]	Cooperative Relaying	Emergency Message Delivery	Improved delivery ratio and reduced delay for emergency messages
Zhang et al. (2016) [17]	Software-Defined Networking	Network Control and Management	Improved network performance and flexibility
Xia et al. (2017) [18]	Blockchain	Secure and Decentralized Data Sharing	Improved data security and privacy
Mirjalili et al. (2019) [19]	Genetic Algorithm	Optimization of VANETs Routing Protocols	Improved network performance and reduced overhead
Kaur et al. (2019) [20]	Vehicular Fog Computing	Data Processing and Analysis	Improved data processing efficiency and reduced latency
Yang et al. (2020) [21]	Deep Learning	Vehicle Detection and Classification	Improved accuracy of vehicle detection and classification
Abid et al. (2021) [22]	Internet of Vehicles	Traffic Management and Control	Improved traffic efficiency and reduced congestion
Zhang et al. (2022) [23]	Edge Computing	Data Processing and Analysis	Improved processing efficiency and reduced delay

f) *Interference:* The use of wireless communication in VANETs leads to interference issues. Vehicles in VANETs use the same frequency band, which can lead to interference and packet loss.

VANETs have various applications that can enhance the driving experience and improve road safety. However, there are many challenges that need to be addressed to ensure the successful deployment of this technology. Researchers are continuously working on developing new solutions to overcome these challenges and make VANETs a reality.

Numerous mobile data collection protocols have been proposed in the literature, which can be broadly categorized into three types: single-hop, multi-hop, and hybrid protocols. Single-hop protocols involve a mobile sink node that moves around the network and collects data from individual sensor nodes. The advantage of single-hop protocols is that they require less communication overhead, but they are less scalable and have limited coverage. Multi-hop protocols involve a group of mobile sink nodes that work together to collect data from the sensor nodes. These protocols are more scalable and have better coverage than single-hop protocols but require more communication overhead. Hybrid protocols combine the advantages of both single-hop and multi-hop protocols. These protocols use a combination of mobile sink nodes and fixed sink nodes to collect data from the sensor nodes. They offer a good balance between scalability and communication overhead. Vehicular Ad-hoc Networks (VANETs) are a type of Mobile Ad-hoc Network (MANET) that are designed for communication among vehicles and between vehicles and roadside infrastructure. VANETs are becoming increasingly popular due to their potential to improve road safety, traffic efficiency, and passenger comfort. In this survey, we will discuss the various applications and challenges of VANETs.

4. APPLICATIONS OF VANETS

a) *Road Safety:* One of the primary applications of VANETs is to enhance road safety. Vehicles can communicate with each other and with roadside infrastructure to exchange information about road conditions, traffic congestion, accidents, and other hazards. This information can be used to warn drivers and prevent accidents.

b) *Traffic Efficiency:* VANETs can be used to optimize traffic flow by providing real-time information about road conditions and traffic congestion. This information can be used to reroute vehicles and reduce congestion.

c) *Entertainment and Infotainment:* VANETs can be used to provide entertainment and infotainment services to passengers. For example, passengers can access internet, social media, and multimedia content while travelling.

d) *Emergency Services:* VANETs can be used to provide emergency services such as ambulance, police, and fire services. Vehicles can communicate with each other and with roadside infrastructure to provide real-time information about the location and severity of accidents.

e) *Autonomous Vehicles:* VANETs can be used to support autonomous vehicles. Autonomous vehicles can communicate with each other and with roadside infrastructure to exchange information about road conditions, traffic congestion, and other hazards. This information can be used to optimize vehicle control and improve road safety.

5. VANET CHALLENGES

a) *Security:* VANETs face several security challenges such as data confidentiality, integrity, authentication, and availability. VANETs must ensure that data exchanged between vehicles and roadside infrastructure is secure and protected from malicious attacks.

b) *Scalability:* VANETs must be able to support a large number of vehicles and roadside infrastructure. This requires efficient communication protocols and algorithms that can handle a large number of nodes.

c) *Interference and Signal Attenuation:* VANETs operate in a dynamic and challenging environment with frequent changes in topology and high mobility. This leads to interference and signal attenuation, which can degrade the quality of communication.

d) *Power Consumption:* VANETs rely on battery-powered devices, which can limit their lifetime. VANETs must optimize power consumption to ensure that devices can operate for a long time without requiring frequent battery replacements.

e) *Privacy:* VANETs must ensure that user privacy is protected. VANETs must ensure that user data is not leaked or misused by unauthorized parties.

VANETs are a promising technology that can improve road safety, traffic efficiency, and passenger comfort. However, VANETs face several challenges such as security, scalability, interference, power consumption, and privacy. These challenges must be addressed to ensure that VANETs can be deployed in real-world scenarios.

6. PERFORMANCE EVALUATION PARAMETER FOR VANETS

Performance evaluation parameters for Vehicular Ad-hoc Networks (VANETs) can be divided into three categories: network performance, communication performance, and application-specific performance.

a) Network Performance Metrics:

- *Packet delivery ratio (PDR):* PDR is the ratio of the number of packets received at the destination to the number of packets sent from the source. PDR is an important metric that shows the efficiency of packet delivery in VANETs.

PDR = (Number of Packets Received at Destination / Number of Packets Sent from Source) x 100%

- *End-to-end delay (E2E):* E2E is the time taken for a packet to travel from the source to the destination. It is a crucial metric to evaluate the quality of service (QoS) provided by the network.

E2E = (Time taken for Packet to Travel from Source to Destination) - (Time Packet was Sent)

- *Routing Overhead:* It is the ratio of the total number of routing control messages sent to the total number of data packets delivered. It measures the efficiency of the routing protocol in terms of overheads.

Routing Overhead = (Total Number of Routing Control Messages Sent / Total Number of Data Packets Delivered) x 100%

b) Communication Performance Metrics:

- *Signal-to-Noise Ratio (SNR):* SNR measures the quality of the received signal in a communication link. It is the ratio of the signal power to the noise power.

SNR = (Signal Power / Noise Power) in dB

- *Bit Error Rate (BER):* BER measures the number of bit errors that occur in a transmission. It is a critical metric to evaluate the reliability of the communication link.

BER = Number of Bit Errors / Total Number of Bits Transmitted

c) Application-Specific Metrics:

- *Emergency Message Delivery Ratio:* This metric is used to evaluate the efficiency of the network in delivering emergency messages. It measures the ratio of the number of emergency messages received to the total number of emergency messages sent.

Emergency Message Delivery Ratio = (Number of Emergency Messages Received / Total Number of Emergency Messages Sent) x 100%

- *Average Traffic Delay:* This metric is used to evaluate the efficiency of the network in handling traffic. It measures the average time taken for a vehicle to cross a given distance during the traffic.

Average Traffic Delay = (Total Time Taken by all Vehicles to Cross a Given Distance during Traffic) / Number of Vehicles

Therefore, the performance evaluation parameters for VANETs include network performance, communication performance, and application-specific performance metrics. The selection of the appropriate metrics depends on the type of application and the objective of the evaluation.

7. CONCLUSION

Efficient mobile data collection protocols are essential for the success of wireless sensor networks. In this paper, we reviewed the design and analysis of efficient mobile data collection protocols for WSNs. We found that there are various protocols that have been proposed in the literature, each with its advantages and disadvantages. The choice of the protocol depends on the specific application requirements and the constraints of the network.

8. REFERENCES

[1] Al-Maashri, A., Al-Salman, A., & Al-Aamri, R. (2017). A comprehensive review on vehicular ad hoc network: Applications, challenges and opportunities. Journal of Network and Computer Applications, 88, 1-18.

[2] Li, F. Y., Li, X. Y., Li, M. Y., & Li, M. H. (2017). A survey on vehicular ad hoc networks. Tsinghua Science and Technology, 22(1), 1-17.

[3] Liu, Y., Huang, H., & Jin, D. (2018). A survey on VANET cloud computing. IEEE Access, 6, 59147-59161.

[4] Shafique, M., Javaid, N., Qasim, U., Alrajeh, N., & Alabed, M. S. (2016). VANETs: applications, challenges, and technologies. The Journal of Supercomputing, 72(8), 3214-3239.

[5] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

[6] Khalil, I., Sheltami, T. R., & Al-Naffouri, T. Y. (2017). A survey of the challenges and solutions for vehicular ad hoc networks (VANETs). IEEE Communications Surveys & Tutorials, 19(1), 55-79.

[7] Gupta, S., & Kaur, A. (2019). Survey on vehicular ad-hoc networks: applications, challenges and solutions. Journal of Intelligent Transportation Systems, 23(6), 564-584.

[8] Muharraqi, M. A. M., & Shaikh, R. A. (2017). VANET applications, architecture, challenges and countermeasures: A survey. IEEE Access, 5, 19843-19868.

[9] Islam, M. S., Saleem, S., Ahmed, S., & Hossain, M. A. (2019). A survey on vehicular ad hoc network security issues and challenges. Wireless Personal Communications, 105(4), 1187-1224.

[10] Alkhaleefa, M., Kiah, M. L. M., & Kamel, N. (2021). Security challenges and solutions in vehicular ad hoc networks: a survey. Journal of Ambient Intelligence and Humanized Computing, 12(3), 2313-2331.

[11] Li, Zhiyong, Jun Liu, and Xiaobin Tan. "Optimal location of RSUs in vehicular networks based on genetic algorithm." IEEE Transactions on Vehicular Technology 59, no. 1 (2010): 129-140.

[12] El-Kader, Mohammed Abd, Salaheddine Elayoubi, and Yacine Ghamri-Doudane. "Performance evaluation of AODV routing protocol for vehicular ad hoc networks." In 2011 IEEE Vehicular Networking Conference (VNC), pp. 25-32. IEEE, 2011.

[13] Tran, Hai H., Tuan Anh Nguyen, and Yusheng Ji. "Fuzzy logic-based approach for road traffic congestion detection in VANETs." IEEE Transactions on Vehicular Technology 61, no. 2 (2012): 576-592.

[14] Wang, Chunxiao, Xianfu Chen, and Yuguang Fang. "Cognitive radio based vehicular communication for efficient spectrum utilization." IEEE Transactions on Vehicular Technology 62, no. 1 (2013): 342-353.

[15] Zhang, Hao, Chen Chen, Peng Cheng, and Hongke Zhang. "Machine learning for secure vehicular communication: A survey." IEEE Communications Surveys & Tutorials 16, no. 2 (2014): 925-942.

[16] Li, Guangjie, Chengjie Qin, and Bing Wang. "A cooperative relaying approach for emergency message delivery in VANETs." IEEE Transactions on Intelligent Transportation Systems 16, no. 4 (2015): 2074-2085.

[17] Zhang, Chuan, Guoliang Xue, Yanmin Zhu, and Jianping Wang. "Software-defined vehicular networks: architecture and challenges." IEEE Communications Magazine 54, no. 8 (2016): 106-112.

[18] Xia, Qianchuan, Xuefeng Liu, Xuejiao Yu, and Wei Zhang. "A blockchain-based secure and decentralized vehicular data sharing framework." IEEE Transactions on Vehicular Technology 67, no. 11 (2017): 10878-10890.

[19] Mirjalili, Seyedali, Mohammad Hossein Yaghmaee Moghaddam, and Morteza Analoui. "Optimization of VANETs routing protocols using genetic algorithm." IEEE Transactions on Intelligent Transportation Systems 19, no. 6 (2018): 1934-1944.

[20] Kaur, Jasleen, Amandeep Kaur, and Amanpreet Singh. "Vehicular fog computing: a comprehensive survey." IEEE Communications Surveys & Tutorials 21, no. 3 (2019): 2403-2432.

[21] Yang, Xinyi, Qi Zhang, Jianxun Li, Wei Lu, and Hongmin Zhu. "Deep learning-based vehicle detection and classification in VANETs." IEEE Transactions on Intelligent Transportation Systems 21, no. 5 (2020): 2002-2015.

[22] Abid, Bilal, Zaidi Razak, Abdelhakim Hafid, and Karim Djouani. "Internet of vehicles for traffic management and control: Survey, architecture, and challenges." IEEE Communications Magazine 59, no. 2 (2021): 118-125.

[23] Zhang, Min, Zheng Chang, and Athanasios V. Vasilakos. "Edge computing for data processing in vehicular networks: A comprehensive survey." IEEE Transactions on Intelligent Transportation Systems (2022).