IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 11 June 2022, accepted 6 August 2022, date of publication 16 August 2022, date of current version 22 August 2022.

*Digital Object Identifier 10.1109/ACCESS.2022.3198656*

TOPICAL REVIEW

# A Comprehensive Survey on Vehicular Networking: Communications, Applications, Challenges, and Upcoming Research Directions

**NEHAD HAMEED HUSSEIN**[1], **CHONG TAK YAW**[2], **SIAW PAW KOH**[2,3], **SIEH KIONG TIONG**[2,3], **(Senior Member, IEEE), AND KOK HEN CHONG**[3]

[1]College of Graduate Studies (COGS), Universiti Tenaga Nasional (The Energy University), Kajang 43000, Malaysia
[2]Institute of Sustainable Energy, Universiti Tenaga Nasional (The Energy University), Kajang 43000, Malaysia
[3]Department of Electrical and Electronics, College of Engineering, Universiti Tenaga Nasional (The Energy University), Kajang 43000, Malaysia

Corresponding authors: Siaw Paw Koh (johnnykoh@uniten.edu.my) and Chong Tak Yaw (chongty@uniten.edu.my)

This work was supported in part by the Universiti Tenaga Nasional under Grant BOLDREFRESH 2025 (J510050002 (IC-6C)).

**ABSTRACT** Nowadays, advanced communication technologies are being utilized to develop intelligent transportation management and driving assistance. Through the ability to exchange traffic and infotainment information between road infrastructure and vehicles, vehicular ad-hoc networks (VANETs) promise to improve transport efficiency, accident prevention, and pedestrians comfort. The deployment of VANETs in the real world is based on the message's correctness and timely delivery and assuredness of privacy protection and data security. In this regard, many researchers have conducted surveys and studies that present models and solutions related to the improvement of VANET from different aspects such as architectural design, networking, and data security. Motivated by these influences, this study presents a detailed survey of VANETs to provide a complete picture of particular VANET applications, networking, and challenges. None of them collected all data in one survey. VANET communication techniques and their improvements are the focus of this study. The contributions of this paper are as follows. First, a complete taxonomy of VANET wireless access techniques has been provided based on various parameters. Second, a detailed discussion and classification VANET services and applications are provided. Third, the challenges related to VANET according to the applicability area, data networking, and resource management are explored in detail. Based on this classification, a complete description of the challenges for each category, including the proposed solutions and development models, is provided to overcome such challenges. Finally, the integration of evolutionary technologies with VANET is comprehensively presented. In this regard, a thorough explanation is provided for each technology, including the challenges, solutions, and suggestions for further improvements. This study enables various users working in the vehicular networking domain to select one of the proposals based on its relative advantages.

**INDEX TERMS** VANET, vehicular communication, safety-related, security, routing, V2V, V2I, V2X.

## I. INTRODUCTION

Currently, cities are densely populated, as more than half of the world is located in towns, and this ratio is predicted to increase. Prediction centers claim that this percentage will be approximately 66% of the world's populace. Governments put on new traffic rules and make many precautions on public roads, but the enhancement rates are still low. With regard road safety, approximately 92 percent of road accidents are often attributed to failures in human recognition (e.g., driver disregard, insufficient surveillance, and drivers distraction) and human decision mistakes (e.g., too fast driving, delayed reactions,and misjudging of the safety distance) [1]. Moreover, even with the development of various safety-oriented

The associate editor coordinating the review of this manuscript and approving it for publication was Kezhi Wang.

techniques in vehicle, such as anti-locking braking systems (ABS), seatbelts, airbags, and rear-view cameras, many people die annually from road traffic accidents [2]. Therefore, the reduction of vehicle accidents and the continuous optimization of transportation system asked urgently to provide a vehicular communication network that enables vehicles to communicate with roadside infrastructure and among them to exchange and share their data, thereby avoiding traffic congestion and leading to the achievement of an intelligent transportation system (ITS). Such networks are called vehicular ad hoc networks (VANETs), which aim to deliver low-latency safety-related messages and infotainment services for both drivers and driverless vehicles [1], [2]. VANET can provide different services such as safety applications, driving assistance, collision avoidance, traffic control, and entertainment services. However, owing to traffic issues that can contribute to fatal results and significant delays for travelers, VANETs developers have given the highest priority to the transmission of critical safety-related information [2], [3].

Initially, onboard units (OBUs) are embedded in vehicles to allow them to communicate directly with fixed roadside units (RSUs) using V2I (Vehicle to Infrastructure) wireless links or among vehicles themselves through V2V (Vehicle to Vehicle) links. Nowadays, the development of the vehicles industry supports the prospect of allowing cars to share and exchange the data with pedestrians' handhelds, bicycles, ground stations (GNs), unmanned aerial vehicles (UAVs), etc. through Vehicle-to-Everything (V2X) communication where the vehicles can communicate and interact with everything around it [2], [3], [4]. As compared with current Ad-Hoc networks such as MANET (Mobile Ad-Hoc Network), FANET (Flying Ad-Hoc Network), and WSN (Wireless Sensor Networks), VANETs have many unique features such as high vehicles mobility, transportation infrastructure dependency, dynamic network change, and intermittent network connectivity. These characteristics lead to several issues and challenges in data delivery and communication reliability [3]. The necessity of reliable communication with low latency and substantial data rates in VANET networks was the reason for a great number of scientists and researchers to study the ability of VANET to cooperate and collaborate with other networks and infrastructures such as cellular networks [5], [6], satellite networks [7], [8], WSN [9], cognitive radio networks [10], [11], [12], and recently UAVs networks [13], [14], [15], [17], [18].

### A. MOTIVATION

The enhancement of the deployment of VANETs has been seen as the basis for the success of a large number of ITS services that require a considerable enhancement in terms of data delivery delay, stable network performance, reliability, scalability, and flexibility. This requires heterogonous cooperation between VANET and other wireless technologies and networking infrastructure such as cellular networks and WSN. The rapid advancement in the vehicular industries, especially in electric vehicles and autonomous vehicles, should take into account many challenges related to both the VANET network and the behavior of such vehicles, to guarantee they are advantageous from ITS services. However, to ensure high reliability and scalability in VANET communication, the following inquiries should be answered carefully:

1) What are the pros and cons of utilizing the VANET network?
2) What are the conditions that make using the VANET helpful network?
3) What are the main challenges that may limit the ITS services?
4) What are VANET services that can be provided, and what are the direct consequences for those services?
5) What are the main wireless technologies that should be used to enhance the performances of VANET?
6) What is the rule of new technologies in the improvement of VANET communication?
7) How can the reliability of VANET services improve with better assist vehicles?

As it's familiar, the precise study of the existing methods and proposals and defining their limits and gaps can constantly help to develop innovative systems and find the best solutions for these limits and gaps. Consequently, and motivated by the abovementioned queries, this paper presents a comprehensive study of the existing techniques and proposals related to VANET networking and communication. It is interested in providing comprehensive details about different methods and paradigms used to improve vehicular communication, such as data routing, traffic load surveillance, network coverage enhancement, monitoring transportation infrastructure, VANET security, etc. Moreover, the challenges and future trends of integration of the new techniques such as federated learning, fog computing, SDN/VNF, 6G, and tactile communication in VANET is widely mentioned here.

### B. RELATED SURVEYS AND TUTORIALS

Nowadays, the number of survey works studying VANET concerns has increased exponentially. However, the authors mainly focused on specific research areas in their surveys, such as data routing, VANET security, SDN-based VANET, and data dissemination. None of them has provided a comprehensive study on the VANET related aspects such as the impact of VANET challenges on different ITS services, the primary wireless technologies that can enhance VANET communication, and the significance of new technologies on the VANET communication enhancement. Table 1 presents a comparative analysis depending on the main points between the common existing surveys related to the VANET network and our survey.

### C. SURVEY ORGANIZATION

To help readers in the navigation of this survey, Fig. 1 provides the survey organization and Fig. 2 presents the detailed structure of the survey. Table 2 contains a list of abbreviations

**TABLE 1.** Comparison of surveys on the VANET network. The symbol √ points to that topic is discussed; the symbol X denotes a topic that has not been discussed, whereas the symbol ∂ denotes a topic that is somewhat covered.

| Year | Reference | VANET Communications | VANET Wireless Access | VANET Characteristics | VANET Services | Comparative Study | Applications Taxonomy | Challenges Classification | Upcoming Technologies Applications | Future Challenges | Proposed Improvements | New Trends | Main Topic |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2021 | 19 | X | X | X | √ | X | √ | √ | ∂ | ∂ | X | ∂ | It provides thorough descriptions of VANETs Cloud, including its architecture, applications, challenges, and issues. |
| | 20 | √ | X | X | X | ∂ | X | ∂ | X | X | ∂ | X | It surveys the evaluation methods of VANET broadcasting protocols. |
| | 21 | X | X | ∂ | ∂ | X | √ | X | X | X | X | X | ML models and techniques for VANET based traffic management |
| | 22 | √ | X | ∂ | √ | X | ∂ | √ | X | √ | ∂ | √ | AI techniques for VANETs communication improvement. |
| | 23 | X | X | ∂ | ∂ | ∂ | X | ∂ | X | X | ∂ | ∂ | Security Challenges of VANET and their current solutions |
| | 24 | ∂ | X | X | ∂ | ∂ | √ | √ | X | X | X | X | The cross-layer methods for VANET communication improvement |
| 2020 | 2 | ∂ | X | X | √ | √ | √ | X | X | X | X | X | VANET services and the main challenges that affect their deployment. |
| | 25 | ∂ | X | X | √ | X | √ | X | X | X | X | ∂ | It details V2V communication system applications |
| | 26 | ∂ | X | X | X | X | X | X | X | ∂ | ∂ | √ | Survey the VANET authentication and privacy-preserving techniques |
| | 27 | X | X | ∂ | ∂ | X | X | √ | ∂ | X | √ | ∂ | It presents the main challenges and existing position-based routing strategies in VANET. |
| | 28 | ∂ | X | X | X | X | X | X | ∂ | ∂ | X | √ | It provides comprehensive details of the applications, challenges, security, recent solutions, and uses for SDN in VANET. |
| 2019 | 1 | √ | X | √ | √ | X | √ | X | X | X | √ | ∂ | It provides details of applications and security issues in IoV/VANET |
| | 29 | ∂ | X | √ | ∂ | X | X | √ | X | ∂ | X | ∂ | It discussed the architecture, applications, issues, and future directions in vehicular edge computing. |
| | 30 | √ | √ | ∂ | X | X | X | X | X | ∂ | X | X | It compares the IoV and VANET through a communication view. |
| | 31 | ∂ | X | √ | X | X | X | ∂ | X | X | X | ∂ | This survey addresses the IoV architectures, networking, and open challenges in vehicular network deployment. |
| 2018 | 32 | ∂ | X | ∂ | X | X | X | X | X | ∂ | ∂ | ∂ | It details the models of QoE/QoS for video communication in VANET |
| | 33 | √ | ∂ | X | X | X | X | ∂ | ∂ | ∂ | X | √ | A survey on heterogeneous VANET network and its issues. |
| 2017 | 34 | ∂ | X | X | ∂ | X | X | X | X | ∂ | X | X | It reviews the role of VANET's protocols in urban safety improvement |
| | 35 | √ | √ | √ | √ | ∂ | X | X | X | √ | ∂ | √ | It summarizes the QoS-aware VANET broadcasting protocols |
| | 36 | ∂ | X | ∂ | X | X | X | ∂ | ∂ | X | X | ∂ | VANET security challenges and solutions |
| 2016-2013 | 3 | √ | √ | √ | √ | X | √ | X | X | X | X | X | VANET architectures, communications, and services. |
| | 10 | ∂ | ∂ | ∂ | X | X | ∂ | ∂ | X | X | ∂ | ∂ | Cognitive radio network with VANET |
| | 37 | √ | √ | √ | √ | ∂ | X | X | X | ∂ | X | ∂ | A vehicular data management |
| | 38 | √ | ∂ | ∂ | √ | X | X | X | X | ∂ | X | ∂ | Architecture, challenges, and solutions for Heterogeneous VANET |
| | 39 | ∂ | X | ∂ | ∂ | X | X | X | X | X | √ | √ | It discusses the different techniques of vehicular data dissemination |

used in the paper. This survey is divided into eight major sections that address the following points.

I. Introduction: this section includes the details of the motivations behind the development of this survey and how it will provide new research prospects for both the readers and researchers. Also, this section presents the organization of the survey.

II. VANET Concept: The basics of VANET networks are deliberated in Section II, which elaborately describes a basic overview, networking, and data transmission techniques. Also, a comprehensive discussion on different characteristics that make the deployment of VANET a challenge is presented here.

III. Ad-hoc Networks Comparative Analysis: In Section III, a deep investigation and comparative study of the different characteristics and applicability of other wireless ad-hoc networks including FANET, SANET, TANET, and WSN according to communication, mobility, stability, and more are presented.

IV. Wireless Access Techniques: In Section IV, some backgrounds with full details about the available wireless access techniques used in VANET networks are detailed here.

V. VANET Services and Applications: In Section V, a detailed description of the services and applications that VANET offers is presented with a comprehensive taxonomy.

VI. VANET Deployment Challenges: Section VI will provide the readers with comprehensive details about the challenges that face VANET deployment through different views and applicability.

VII. Future Research Directions: Section VII will include clarifying open challenges, issues, and upcoming research directions. The suggested solutions and recommended references for more investigation are listed here.

VIII. In Section VIII, the study conclusions will be presented.

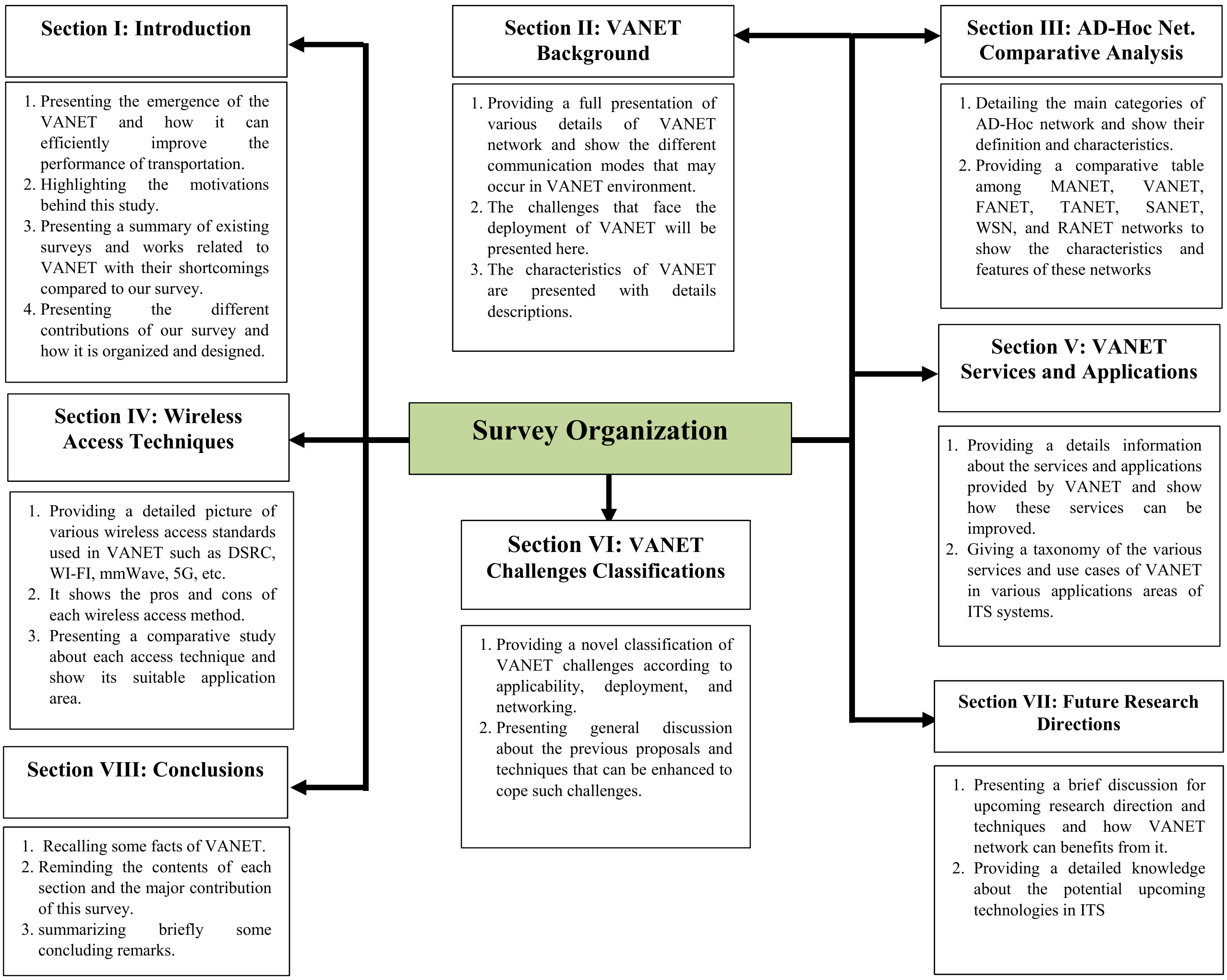



**FIGURE 1.** Organization of the survey.

### D. OUR CONTRIBUTIONS

The contributions of this work can be outlined as:

1) Provision of classification of VANET services and applications with a detailed discussion about all services.
2) Presenting different wireless techniques used in the data communication within the VANET network.
3) Provision of an overview of the VANETs in-depth discussions on the main challenges and constraints of their deployment.
4) Summarizing the survey by both deliberating the various new research challenges and providing proposals with suggested references to address them. Also, some different visions at the conclusion of this work are emphasized here.

## II. VANET BACKGROUND

### A. VANET COMMUNICATIONS

The progress in public transportation systems around the world, whether for commercial or personal purposes, has led to the emergence of many urgencies to develop Intelligent Transportation Systems or VANET [40], [41], [42], [43], [44]. However, according to the latest statistics, the number of cars around the world is 1 billion, and the number may exceed that to be 2 billion in the year 2035 [1], [43], [45]. In VANETs, real-time road conditions or safety-related data can be shared wirelessly among vehicles directly or through other mediums such as passengers' handhelds, RSUs, UAVs, etc. Traffic accidents and road jamming can be efficiently avoided [46]. Moreover, VANETs can share other entertainment information such as news, gaming, and Internet access, which can add fun to the long trip [44]. Consequently, VANET improves drivers' experience and decreases traffic accidents and congestion.

To be part of VANET, vehicles should be enhanced with sensors and navigation systems such as GPS, multimedia devices, and wireless modules. Sensors and multimedia techniques can be used to sense the environment and detect the objects around vehicles, such as other vehicles, obstacles, and passengers, to avoid accidents or sudden breaks. On the other hand, the wireless communication modules provide different

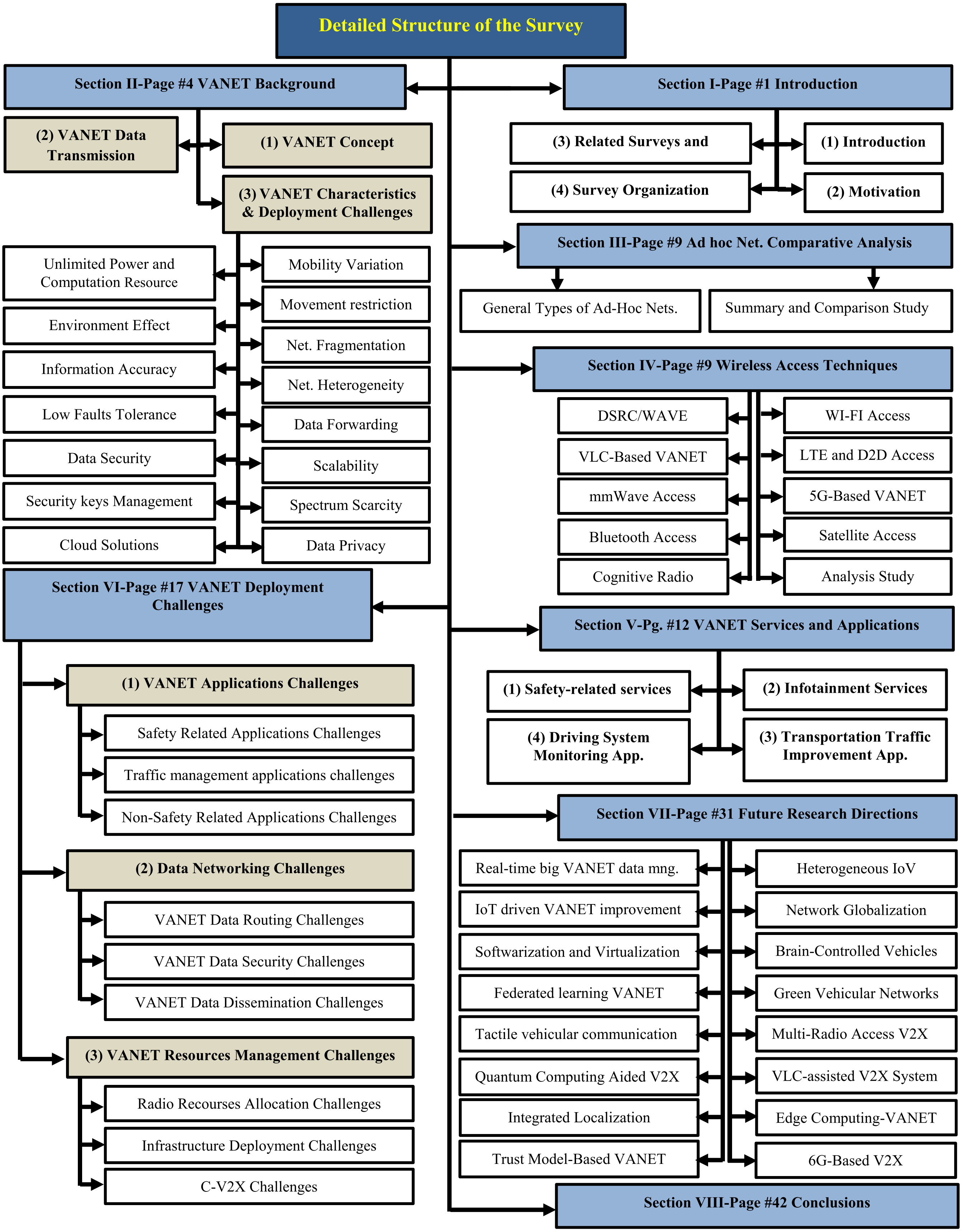



**FIGURE 2.** The detailed structure of the survey.

**TABLE 2.** List of abbreviation.

| Acronym | Definition |
|---|---|
| ABS | anti-locking braking systems |
| ITS | Intelligent Transportation System |
| OBU | on-board units |
| RSU | roadside units |
| V2I | Vehicle to Infrastructure |
| V2V | Vehicle to Vehicle |
| UAV | unmanned aerial vehicles |
| V2X | Vehicle-to-Everything |
| VANET | Vehicular Ad-hoc Network |
| MANET | Mobile Ad-Hoc Network |
| FANET | Flying Ad-Hoc Network |
| RANET | robot ad-hoc networks |
| TANET | train ad-hoc networks |
| SANET | ship ad-hoc networks |
| WSN | Wireless Sensor Networks |
| QoS | Quality of Service |
| QoE | Quality of Experience |
| QoPE | quality of physical experience |
| V2P | Vehicle-to-Pedestrian |
| V2B | Vehicle-to-Barrier |
| V2C | Vehicle-to-Cloud |
| V2U | Vehicle-to-UAV |
| I2I | Infrastructure-to-Infrastructure |
| HRLLC | high rate low latency communications |
| V2S | Vehicle-to-Sensor |
| DSRC | Dedicated Short Range Communication |
| WAVE | Wireless Access in Vehicular Environment |
| WPT | wireless power transmission |
| eMBB | enhanced mobile broadband |
| SSN | self-sustaining network |
| GHG | Green House Gas |
| SDVN | Software-Defined Vehicular Network |
| SDN | Software-Defined Network |
| SDP | software-defined perimeters |
| 4G/LTE | Fourth Generation/Long-Term Evaluation |
| 5G | Fifth Generation |
| ETSI | European Telecommunication Standards Institute |
| FCC | Federal Communication Commission |
| SCH | Service Channel |
| CCH | Control Channel |
| MAC | Medium Access Control |
| VLC | Vehicular Light Communication |
| EV | Electric Vehicle |
| GVRP | Green Vehicle Routing Problem |
| LiDAR | Light Detection and Ranging |
| LOS | Line of Sight |
| MIMO | Multiple Input Multiple Output |
| MEC | Multi-access Edge Computing |
| 5GAA | 5G Automotive Association |
| OTFS | Orthogonal time-frequency space |
| NFV | Network Function Virtualization |
| WBSN | wireless body sensor network |
| FLVN | Federated Learning-Based Vehicular Network |
| TL | Transfer learning |
| URLLC | Ultra-Reliable Low Latency Communication |
| BCV | Brain-Controlled Vehicle |
| ILAC | integrated localization and communication |
| IoT | Internet of Things |
| IoV | Internet of Vehicles |
| CIOT | Consumer IoT |
| BCI | brain-computer interface |
| KPI | key performance indicator |

types of communication links that can be categorized according to the communicating entities in [47], presented in Fig. 3.

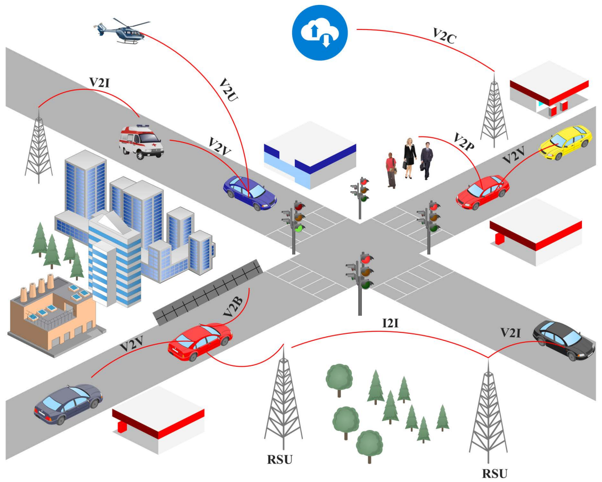



**FIGURE 3.** Basic VANET communications.

1) Vehicle-to-Vehicle (V2V) communications occur directly among vehicles without any infrastructure. These links are mainly used to share safety-related information.
2) Vehicle-to-infrastructure (V2I) communications allow vehicles to share sensing data with roadside infrastructures such as roadside units (RSU) or cellular base stations. These links also can be used to share announcements and provide Internet access.
3) Infrastructure-to-infrastructure (I2I) communications are used to share global road traffic information among infrastructures in specific areas.
4) Vehicle-to-Pedestrian (V2P) communications are used to share data with handhelds devices around vehicles.
5) Vehicle-to-Barrier (V2B) communications are required to share data with the roadside barriers [48]. This communication benefits from a massive number of sensors in vehicles to avoid run-off-road accidents.
6) Vehicle-to-Cloud (V2C) communication allows RSUs and cloud servers are communicated for several tasks, such as data analysis, decision making, and transportation prediction [49].
7) Vehicle-to-UAV (V2U) communication, in this type, the data are transferred wirelessly between the vehicles and UAVs through Ground to Aerial links.
8) Vehicle-to-Sensors (V2S) communication, through V2S, the vehicles and embedded sensors will exchange the sensing data of the road and surrounding environment.

VANET is a tremendously extensive wireless network that spreads across whole transportation systems. The high mobility of vehicles and diverse distribution of roads are the main reasons for the dynamicity of the VANET network topology. For optimal results, VANETs communications must be adapted to the dynamic nature of the VANET and the different QoS requirements for provided services. On the other side, many applications require numerous QoS requirements. For instance, the safety-related services should be accessed with low latency and high reliability, while the non-safety-related applications require links with high throughput [50].

### B. DISTINGUISHED CHARACTERISTICS OF VANET

VANET networks have some characteristics and challenges that make the provision of services and ensuring their reliability complex and multi-metric dependent issues. Some of these characteristics are explained here.

1) Mobility Variation: In the VANET network, the communicating entities can be stationary (e.g., RSUs), slow-moving vehicles (e.g., vehicles in traffic jams and road intersections), or moving entities with high speeds such as vehicles on sparse and highways roads. This variation in nodes mobility has brought various challenges to VANET communication. For instance, in the high-velocity scenario, the opportunity for successful communication between VANET entities will be small because of the minor transmission range [53]. Similarly, in a moderate velocity scenario, the VANET communication will be degraded due to the Doppler effect, numerous link breakages, and increased end-to-end (E2E) latency [54], [55]. Also, for the dense environment scenario, although there is a high ability for data transfer, there are many issues associated with increased road traffic density, including common data collision, bandwidth scarcity, channel fading, packet dropping, and signal interference issues [1].
2) Movement Restriction: In the VANET environment, the vehicle's movement is restricted by the infrastructure of the public transportation system. The roads distribution is different from one city to another. Moreover, roads nature is different according to the underlying area. For instance, the roads in an urban environment will have a high density in terms of vehicles, constructions, and other obstacles compared to those in rural or highway environments. These distinctions in roads distribution will present some problems for reliable data transmission [3].
3) Frequent Network Fragmentation: The vehicle's density may vary according to the time and place; for example, at intersections and roads near workplaces and markets, the density is high. Also, the density is typically high in the daytime compared to the evening time. The density and mobility of VANET nodes will have a high impact on the VANET network fragmentation. The network will suffer from several fragmentations as the density of the node decreases, which negatively affects the continuity of the communication and packets forwarding [54]. Moreover, moving the vehicles at high velocities will increase the dynamicity of the VANET topology. Due to this, the VANET network may be fragmented into several separate pieces [3].
4) Heterogeneity: the VANET network comprises many nodes that differ in terms of properties and applications. These nodes may be fixed, such as RSUs, or movable, such as vehicles. Also, some vehicles require infotainment data exchange, and some require safety-related data exchange. Moreover, manufacturers set many restrictions that restrict the data transfer and sharing processes. For instance, autonomous vehicles manufacturers may place more restrictions on the privacy of the vehicle's data [1]. As a result, a VANET system should deal with the heterogeneity of nodes and services. Moreover, conventional routing methods use routing tables to find the routing information of the next hop toward the data destination. However, because of the high degree of vehicles mobility and topology dynamicity in the VANET environment, routing data packets through these types of protocols will cause degraded performance, particularly in a highly dynamic environment [56]. So, For the best results, the routing protocol should be adapted to traffic density and network topology changes. If the traffic is dense, the protocol should have the ability to select the link with minimum delay. On the other side, if the traffic is sparse, the vehicle can be used as a store-carry-forward relay. This can ensure data delivery but increase the delay.
5) Scalability: In VANET, the communication can be one urban, more than one urban, or large cities and countries. Hence, the size of the VANET network may be unlimited geographically network. Scalability is one of the main challenges in vehicular communication [57]. This means the performance of the VANET communication must be reliable even when the number of communicable nodes is small [54]. Thus scalability means the network can scale or adapt for future growth and changes. This is practicable if the system can find the location information for each node and use this information in the data forwarding strategy [58]. This eliminates the need for knowing the network topology of the VANET, thus decreasing the control messages overhead. Nowadays, Using UAVs represents a new prestigious solution for scalability issues in the VANET network by using them as direct or store-carry-forward data relays [5].
6) Unlimited Power and computation resources: The power and storage don't represent any restrictions on the nodes' communications in the VANET network. In VANET, OBUs are embedded in vehicles operating with continuous unconstrained power sources from vehicles' batteries so that there are no issues with power and processing resources. This supports to execution of different power-consuming techniques such as RSA and ECDSA techniques [59].
7) Spectrum Scarcity: The wireless technology standards for vehicular networks include dedicated short-range communication (DSRC) and wireless

access in vehicular environments (WAVE). The latest investigation studies of the DSRC-based VANETs have recognized their reliability and scalability issues in large-scale dense vehicular networks [10], [12]. One of the main reasons for these reliability and scalability problems is insufficient and scarce frequency channels for vehicular communication systems. The seven DSRC channels are periodically utilized by all vehicles for their data communication. This means that all vehicles will need to contend for these channels to transmit vehicular data packets. As a result, this channels competition may lead to network congestion, maximize packet delay, and reduce throughput, causing to degrade the QoS as a whole [46].

8) Environmental Effect: In VANET, all communications take place outdoor, where the effect of the surrounding environment on the electromagnetic signals will be relatively large. These signals are propagated in the air and may be conflicted by the buildings, vehicles, trees, etc., causing different signal impairments like multipath propagation, channel fading, and signal shadowing [60]. Also, the weather changes will affect the high-speed and low latency data communication in VANETs. For instance, rainy weather, icy weather, and snowy weather will affect the conductivity of the surfaces, which causes many effects on the reflection paths and, accordingly, degrade the performance of data communication in the VANETs network. These conditions can make the roads saturated with water or accumulate snow, which negatively affects multi-hop communication in the VANET network. Dusty weather will cause diverse effects on the communication of VANETs. Sandy grains will result in high attenuation in the microwave signals, which will affect the performance of data transfer in VANETs [61].
9) Information Accuracy: Many methods for data delivery in VANETs environment use the positional information obtained over navigational systems such as GPS and GNSS [62]. Unfortunately, these systems cannot provide accurate position information [63]. For instance, the buildings and underground tunnels will cause blockage in GPS signals. Also, its power may be degraded by the atmospheric effect from the troposphere and ionosphere. As a whole, in the optimal scenario, the GPS signal accuracy may be from 5 to 30 m in a dense urban region. This accuracy is small and may cause numerous issues in the reliability of low-latency VANET services. On the other side, RSU will collect data on current vehicles within the area it covers. This information may be delivered to the cloud or SDN to analyze it and make future decisions. Due to the vehicle's high speed and continuous movement, this information may be inaccurate and needs to be updated, which causes an error in the analysis and the correct decision-making [59].
10) Low Faults Tolerance: Real-time communication represents the primary requirement for various safety-related services in the VANET network. However, any faults or errors may cause an additional delay in data delivery, resulting in traffic congestion and severe disasters. To avoid such situations, preemptive security actions should be achieved on time, allowing the drivers to take action proactively if any emergency state occurs [64], [65].
11) Data Security: Management–effective and reliable communication requires data to be delivered in a secure manner [66]. Data destination should ensure the packets are not changed during their transmission. Also, it must be encrypted so that no intruder can detect it and eavesdrop on its content. Finally, it should be made sure that it was sent from the sender and not from a third party. Security is a vital issue in VANETs deployment since if the network is hacked, the vehicles can undoubtedly be managed by hackers, leading to traffic mistakes and fatal disasters. However, due to VANET characteristics such as the dynamic network topology and vehicles mobility, data security and non-repudiation are essential challenges in VANET deployment [67]. Also, keys are the vital entities in cryptographic algorithms used to encrypt and decrypt critical life information in the VANET environment. The frequent changes in VANET network topology make the keys management a big challenge [66]. However, any method suggested for VANET security enhancement should take into account how the keys are generated and distributed [44]. Key Revocation is one of the central parts of the key management that is the method of neglecting the keys of the malicious subscribers. Consequently, the VANETs network topology's extendibility may result in a large list of revocable keys, which maximizes the overhead of the keys revocation procedure [66].
12) Data privacy: Many people do not want to share information related to their vehicles or that can be used to find out where they intend to go. Thus, data privacy has become one of the most important problems that require a balance between high privacy and people's desire [68], [69].

## III. COMPARATIVE ANALYSIS

In wireless ad-hoc networking, MANETs can be further classified into wireless sensor networks (WSN), robot ad-hoc networks (RANET), flying ad-hoc networks (FANET) train ad-hoc networks (TANET), and ship ad-hoc networks (SANET) as shown in Fig. 4. This classification depends on the type of communicating entities and the deployment environment of these entities [70]. However, each of these classes has its features, faces distinctive challenges, and works with many concerns. Table 3 enhances this survey by providing the characteristics of each network [13], [14], [15].

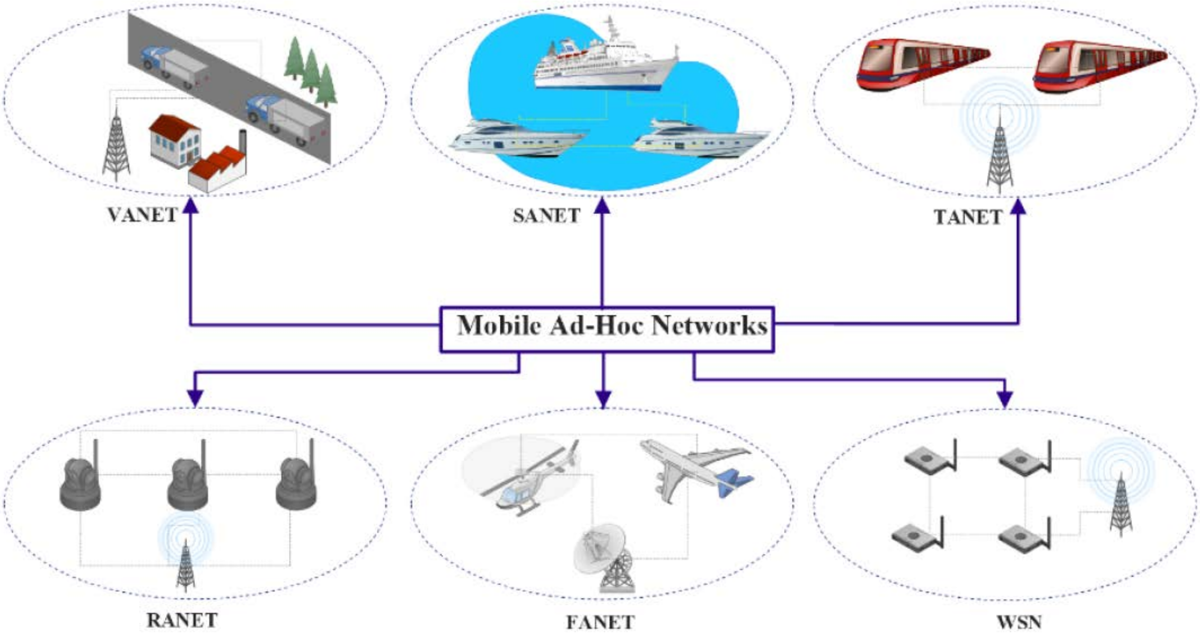



**FIGURE 4.** Different classes of MANET network.

WSNs are a group of small and low-cost sensing devices that can sense data from a nearby location and directly transfer it to a central unit, called a Sink. WSNs can be used in various industrial, housing, and civil domains [71]. However, the nodes in WSN are distinguished by static or low mobility features, and their density in almost all cases is low. Also, the power supplies in such nodes represent one of the main challenges in WSN deployment.

FANET networks consist of a group of UAVs and as a minimum one of them should be communicated with ground base stations (GBS) or satellites [15]. The UAVs formed a specific FANET can cooperate and collaborate through inter-UAV wireless links. Generally, the FANETs require further advanced software and hardware systems for UAVs coordination, management, and communication [14], [17]. FANETs networks require efficient nodes coordination systems to avoid their collisions.

RANETs networks consist of robots in a specific area. These robots should exchange the sensing data to other reports or centralized units to enhance their work or avoid collisions with obstacles and other robots. [72]. Generally, robots' mobility is restricted, and they can move intelligently. Also, the robots have limited energy capacity, which enforces intelligent management of their power consumption.

SANETs are extensive networks used to provide the coverage of nautical communication among ships [73]. These networks suffer from signal propagation delay, frequent network disconnectivity, and nodes' low density.

## IV. WIRELESS ACCESS STANDARDS OF VANET

The cooperation of various communication and information technologies in vehicular networks causes high heterogeneity in VANET. There are multiple categories of communication, such as Inter-vehicular communication, intra-vehicular communication, and vehicle-infrastructure communication [74]. In the beginning, VANETs were mainly dependent on DSRC to provide vehicular communications. Still, the bandwidth scarcity in this standard and the high potential of traffic congestion and increased delays pushed researchers to more comprehensive ideas.

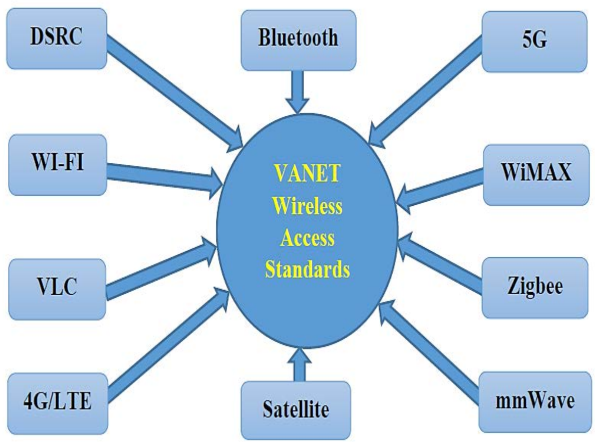



**FIGURE 5.** Wireless access standards used in VANET communication.

Moreover, the increase in services provided by VANET and the necessity to ensure continuity and scalability of VANET communication have motivated the utilization of different types of wireless communications (as shown in Fig. 5) such as cellular communication (4G/LTE), short-range static communication (Zigbee, Bluetooth, and Wi-Fi), Ultra-Reliable and

**TABLE 3.** Comparison of different categories of MANET network [13], [14], [15].

| | VANET | FANET | SANET | TANET | RANET | WSN |
|---|---|---|---|---|---|---|
| **Node Type** | Car, Saloon, Van, Bus, Bike, Lorry | Drone, Airplane, Copter, Satellite | Ship, boat, underwater vehicles, USV (Unmanned Surface Vehicles), vessels | monorails, railway, atmospheric, railway high-speed, rubber-tired underground, and cog railways. | Robots | Sensors |
| **Node Speed** | Medium to High, depending on roads (Avg. 20-130 Km/h) | Low to High (Average 6-460 Km/H) | Medium to High (Avg. 20-130 Km/h) | Low to High (Avg. 5-550 Km/h) | Static to medium (Avg. 0-20 km/h) | Static to lower (Avg. 0-6 km/h) |
| **Node Density** | Low to high depends on tempo spatial | Low, depends on the application | Medium | Low | Low | Low, depends on the apps. |
| **Node Mobility** | Regular 2D Predefined or random trajectories | Free 3D Predefined or random trajectories | Free 2D Predefined trajectories | Regular 2D Predefined trajectories | Free 2D or 3D Controlled trajectories | Static or low 2D or 3D Predefined trajectories |
| **Coverage** | Medium | Low | Medium | Low | Low | Low |
| **Topology Change** | Fast | Fast | Slow | Low | Slow | Slow |
| **Propagation Mode** | On the Ground Low LoS | In the air High LoS | On the water High LoS | On the Ground Low LoS | On the ground Low LoS | On the ground Low LoS |
| **Fixed Infrastructure** | RSUs | GBS | Controller | Controller | Controller | Sink |
| **Lunch System** | Roads | Hands Airfield | Water | Ground, underground, or hanging in the air rails | Placement | Placement |
| **Connectivity** | Low to High | Low to High | Low | Low | Low | Medium |
| **Energy Autonomy** | High | High (depends on the UAV) | High | High | Low | Low |
| **User Interface** | Traffic monitoring | Mission progress | Data Transmission | Traffic monitoring | Data analyzing | Data gathering |
| **Localization** | GPS/AGPS/DGPS,/ GNSS | GPS/AGPS/DGPS/GN SS/IMU/Net/ Height | GPS/AGPS/DGPS/GN SS/ISU | GPS/AGPS/DGPS,/ GNSS | GPS | GPS |
| **Wireless Technology** | IEEE 802.11p | IEEE 802.11a/b/g/ac/s/n/p | IEEE 802.11a/p | IEEE 802.11p | IEEE 802.11 | IEEE 802.15.4 |
| **Frequency Band** | 5.9 GHz | 2.4/5 GHz | 5/8 GHz | 5.9 GHz | 2.4 GHz | 2.4 GHz |
| **Bandwidth Requirements** | Low to High | the required bandwidth is directly proportional to the number of UAVs. | Low | Low | Low to High (based on functionality) | Low |
| **Delay Tolerance** | Minimum | Minimum | Average | Average | Minimum | Average |

low latency communications (5G, MmWave, VLC), satellite communications, and cognitive radio communications.

## A. STANDARD VANET WIRELESS TECHNOLOGY

The significance of vehicular communications paves the academic world and government agencies to realize and standardize vehicular networks. In 1999, US Federal Communications Communication (FCC) prepared the initial standardization process by assigning 75 MHz of dedicated short-range communication (DSRC) spectrum mainly to accomplish V2V and V2I. Likewise, in 2008, the European Telecommunications Standards Institute (ETSI) had assigned 30 MHz in the 6-sub GHz band for vehicular communications [75].

As presented in Fig. 6, DSRC bandwidth has been distributed to 7 channels, each with 10 MHz: six of them are called service channels (SCH) used to transmit safety and non-safety-related packets, and one control channel (CCH) is used for broadcast the control data and critical safety messages.

For more flexibility and adaptability, IEEE approved the DSRC standard entitled Wireless Access in Vehicular Environment (WAVE) in 2003 to make direct vehicular communications at regular road speeds at the range of 1 km [75]. WAVE involves a set of particular standards which contain two primary standards: IEEE 802.11p to achieve the physical and medium access control (MAC) and IEEE 1609 to manage higher-layer processes [76].

Even though the DSRC/WAVE standards in a licensed bandwidth results in a small transmission delay, DSRC/WAVE causes a significant overhead and high delay due to the high mobility of vehicles and the dynamicity of VANET topology. The seven DSRC channels are periodically utilized by all vehicles for their data communication. This means that all vehicles will need to contend for these channels to transmit vehicular data packets. As a result, this channels competition may lead to network congestion,

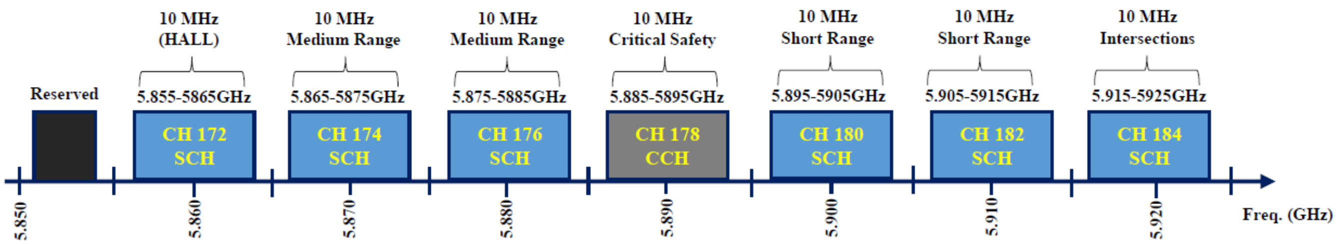



**FIGURE 6.** DSRC spectrum band channels.

maximize packet delay, and reduce throughput, causing to degrade the QoS as a whole [76].

### B. WI-FI BASED VANET

Wi-Fi is the most widespread data communication technology. Because of its acceptable cost, higher data rate, and flexibility, many Wi-Fi or WLAN standards such as IEEE 802.11(a/ac/b/e/g/n) can provide good V2V and V2I data results transmission [77].

Wi-Fi activates in 2.4 and in 5.4 GHz frequency and can provide different data rates such as 11 Mb/s in IEEE801.11b, 54 Mb/s IEEE801.11a and 1 Gigabit/s in IEEE802.11ac. In the dense environment, the requirement for wireless access will rise, causing more overload on the access points and high network congestion with more delay. To overcome this limitation, more access points can be deployed. This will increase complexity and costs. Also, because WI-FI can serve a small coverage area, the high mobility of vehicles will lead to frequent handover and more disconnections [78].

The latest version of Wi-Fi technology is Wi-Fi 6 or IEEE 802.11ax. ABI Research expects extensive adoption and integration of Wi-Fi 6 technology in the vehicular manufacturing. These expectations infer from that nearly 50% of the Wi-Fi chipsets will operate in Wi-Fi 6 at 2023 [64]. Wi-Fi 6 handles signal congestion through utilizing orthogonal frequency division multiple access (OFDMA) and Basic Service Set (BSS) techniques. On the other side, Wi-Fi 6E (5.925-7.125 GHz) represents a vast advance over Wi-Fi 6. Wi-Fi 6E operates at a dedicated 6E spectrum with up to seven additional 160 MHz channels while Wi-Fi 6 operates at only two 160 MHz channels. This allows Wi-Fi 6E techno-logy to offer gigabit speeds more easily [78]. However, due to the prestigious advancements of Wi-Fi 6 and Wi-Fi 6E in terms of bandwidth efficiency, data rates, flexibility, and outdoor coverage, they will be used in inter-vehicular communication for autonomous vehicles over former Wi-Fi versions [64].

### C. VLC BASED VANET COMMUNICATION

In 2012 IEEE invented a new standard called IEEE 802.15.7 based on Visible Light Communication (VLC). VLC provides short-wavelength optical wireless communication by utilizing 380 to 780 nm visible light bands. VLC mostly operates in infrared (IR), visible light, and ultra-violet (UV) bands and frequency ranges in 430–790 THz [79]. However, adopting VLC in vehicular communication can bring many benefits as compared with DSRC based vehicular communication. For instance, the consequence of interference with other electromagnetic signals is almost slight, the E2E delay is smaller, further bandwidth channels are available, and it is less vulnerable to security attacks [80].

Consequently, VLC can be utilized in different V2V and V2B communications, such as lane change decisions, road sense, and traffic indicating [81]. Conversely, the basic characteristics of VLC make its application in VANET a huge barrier. VLC should have occurred through LOS communication, it bases on a very short-range wave, it suffers from signal shadowing, and the weather changes can produce high degradation in VLC data communication [80].

### D. LTE AND DEVICE-TO-DEVICE (D2D) VANET COMMUNICATION

The third-generation partnership program (3GPP) presented Long-Term Evolution Advance (LTE-A) based V2I and device-to-device (D2D) communication for the V2V for providing high data rates [81]. LTE can provide a high data rate, minimized latency, great coverage region, and excellent penetration ability [82]. The maximum data rate provided is 100 Mbps, and the E2E delay cannot be lower than 100ms [83].

However, LTE-based VANET restricts the communication only to V2I and needs special deployment infrastructure for data transmission. Also, in a dense environment, LTE-based VANET communication copes with the limitations of network capacity and congestion problems due to the competition with the conventional application of LTE in the operational environment [83], [84].

On the other hand, the D2D is standardized for ad-hoc V2V communication. D2D communications are based on multi-hop communication to maximize spectrum efficiency and decrease transmission delay [81]. However, the high mobility and regular topology changes will make getting consistent V2V communications a significant challenge [81].

### E. MMWAVE BASED VANET COMMUNICATION

The previously mentioned types of VANET communication can't continuously satisfy the communication restrictions featured by minimum latency and high data rates services that should be used for upcoming ITSs. LTE or D2D can transmit the data with100 Mb/s while DSRC can do that with 3-27 Mb/s as maximum data rates [83]. Moreover, new technologies such as edge computing and fog computing cannot be utilized efficiently because of the restrictions on bandwidth resources [82].

Nowadays, the VANET developers go towards using mmWave in vehicular communication. Due to its operation in high bandwidth (from 30 GHz to 300 GHz), mmWave can provide high data rates exceeding 1 Gb/s in V2V data transmission [84]. mmWave can provide reliable V2V communication to transmit HD camera data, LiDAR sensors, and more. Conversely, mmWave requires LOS communication links and suffers from high penetration loss, bad deflection, and high interference with nearby electric towers and cellular infrastructure [85], [86]. All of these lead to high limitations in the applications of mmWave in high mobility and dense vehicular environments.

### F. 5G COMMUNICATIONS FOR VANET

As clarified previously, LTE is one of the successful technologies that it will carry out in the VANET network. Consequently, it is expected that 5G will be the successor of LTE in VANET communications [87]. In VANET, the latency for the safety message transmission must be up to 100 ms in traditional VANET communication and 1 ms for the connected autonomous vehicles.

However, through Multi-access Edge Computing (MEC), 5G can support reaching such low and ultra-low delays [87]. Moreover, network slicing technology can divide the VANET network into two logical networks, one for the safety-related services and another for the infotainment services. This can ensure high QoS requirements for each type of data communication. To encourage the integration of 5G and VANET communication, the 5G Automotive Association (5GAA) was founded in 2016 [85]. 5GAA has announced that the Cellular-V2X (C-V2X) will be the 5G enabler in VANET communications [88], [89].

The full deployment of 5G-based C-V2X will be realized in the next few years because it requires more development and provisions [90]. However, as compared with LTE, 5G can provide higher data rates reaches to 20 Gb/s, lower latency reaches 1 ms for devices like AV that use Ultra-Reliable Low Latency Communication (URLLC), and greater network capacity due to it operates in higher frequency bands (mmWave bands) [91].

However, cellular networks (LTE/5G) have many weaknesses compared to the DSRC communication, which includes:

1) DSRC can be used in V2V communication without2 infrastructure deployment, but the network infrastructure is central in cellular communication.
2) DSRC based VANET requires much more inexpensive infrastructure than the cellular network infrastructure.
3) While other network participants (User Equipment (UE) or smartphones) share cellular frequency bands in cellular communication, the DSRC frequency channels are allocated entirely to VANET users.

### G. BLUETOOTH FOR VANET

Bluetooth is known as one of the best technologies used in short-range communications. Bluetooth 5 is the recent version of Bluetooth that works in 2.4 GHz to 2.4835 GHz like the former Bluetooth versions but with a higher data rate of 2Mb/s and a wider coverage area (200 m) [92]. Bluetooth can be utilized in VANET communications [93].

Primarily, Bluetooth is being used in intra-vehicle communications such as infotainment services, mobile calls, navigation services, and more. Moreover, its characteristics like low cost, small power consumption, reliable and acceptable delay make it dominant in the V2V and V2I data transmission [94]. Nevertheless, the low data rate and the short coverage area are two primary limits of Bluetooth for the utilization in VANET communication.

### H. SATELLITE COMMUNICATIONS FOR VANET

Alternative possible wireless technology for VANET is satellite communication. Due to its wide coverage area, higher frequency band (90 MHz), and scalability, satellite radio is used in data broadcasting and as the backup wireless access method if cellular communication can never be satisfied. Satellite communication can enhance GPS reliability or provide V2V communication [8].

Also, there are various satellite communication applications in VANET, such as sensor data share, cloud communication, universal tracking, real-time vehicle monitoring in isolated areas, and so on [57], [95]. However, satellite communications cope with severe latency and require a big antenna size. These concerns result from an incompatibility for the satellite in the VANET communications. But, it can provide good results if it is integrated with other wireless infrastructures such as LTE and 5G [95].

### I. ZIGBEE BASED VANET COMMUNICATION

IEEE 802.15.4 Zigbee standard receives special attention from VANET communications due to its suitability for dynamic networks. IEEE 1609 standard can be used to support IEEE 802.15.4 through refining network functions, multichannel abilities, and network management in vehicular communication [40].

Zigbee is explicitly designed to help sense, track, and control requirements that need the least amount of power [42]. Also, Zigbee can assist various low-energy devices demanding time-critical, moderate transmission rate, N-LoS operation, and reliable data transmission in ITS.

Compared with other wireless standards, Zigbee communication is more straightforward and low-priced than Wi-Fi and Bluetooth wireless acess technologies. However, due to its small data rates, Zigbee is not appropriate for infotainment data transmission such as Video communication, file downloading, and VoIP.

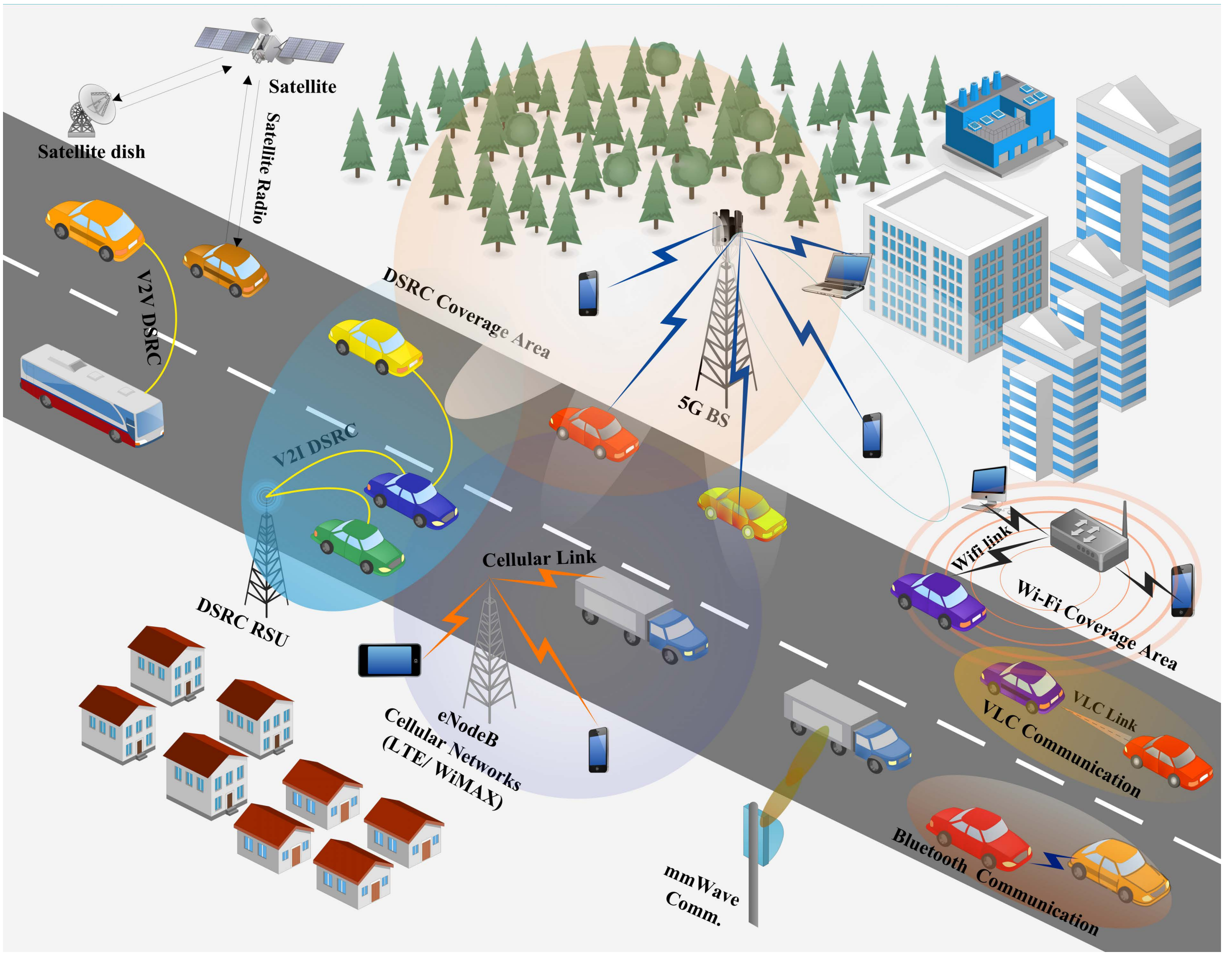



**FIGURE 7.** Wireless access standards for the VANET.

### *J. WIMAX BASED VANET COMMUNICATION*

WiMAX is centered on the IEEE 802.16 standard. The primary objective of WiMAX is to support consistent wireless connectivity over long distances using various methods, ranging from point-to-point to mobile-centric techniques [40]. The mobile-centric WiMAX, known as IEEE 802.16e, allows mobility as per user needs. WiMAX provides reliable, long-range data transmission and high-speed data rates for the VANET network. Hence, it can be efficiently used for V2I or I2I communications.

Fig. 7 shows different wireless access standards in the VANET network. Table 4 presents the comparisons of the wireless access techniques described previously. Still, additional studies are required in these areas, particularly in integrating many standards into a single system. Cognitive radio is a powerful technique for enabling this integration.

## V. VANET APPLICATIONS AND SERVICES

The high demands of the adopting ITS services in smart cities have motivated the acadamia and industries to develop multiple VANET services and applications. Consequently, there are many services and applications that VANETs can offer for government agancies, drivers, and travelers. These services and applications can be classified according to their applicability into safety-related, infotainment, traffic improvement, and driving system monitoring applications [96]. Each of these categories includes many uses and applications. Fig. 8 shows the taxonomy of VANET services and different applications under each category.

### *A. SAFETY-RELATED APPLICATIONS*

Safety-related applications represent the primary services of VANETs provided to bypass and decrease the number of road accidents. Safety data should be generated and transmitted with minimum delay and be provided proactively to allow the driver to make decisions in advance with a warning, and hence, the end to avoiding or reducing the damage of the traffic accidents [97], [98], [99]. Such applications can be categorized into three classes: driving assistance applications, safety information provision applications, and driver warning applications. One of the primary services provided under this category is the intersection collision avoidance system that emphaizes reducing the number of accidents occurred in roads intersection [100]. VANET infrastructure provides the

**TABLE 4.** Comparison of wireless access technologies for the VANET.

| Access Technique | Operating Frequency | Bandwidth | Coverage | Data Rate | Advantages | Disadvantages | Uses |
|---|---|---|---|---|---|---|---|
| DSRC | 5.8-5.925 GHz | 75 MHz | ~1 Km | 27 Mbps | • Wide Coverage<br>• VANET Dedication<br>• Not high Costs<br>• Not more infrastructure | • Scarcity of spectrum<br>• Low transmission power<br>• More latency<br>• Less reliable in highly dynamic transportation | V2V, V2I, V2P |
| WI-FI | 2.4/5 GHZ | 21-2440 MHz | ~100 m | 11/54/600/ 1000 Mbps | • Free license<br>• Large data rate | • Short coverage<br>• Low mobility<br>• Complexity for large scale deployment | V2V, V2I, I2I, V2U, V2P, V2C |
| VLC | 430-790 THz | .. | ~40 m | 2-400 Mbps | • No EMI Effect<br>• High data rate | • Shorter range<br>• Shadowing problem<br>• LoS requirements | V2V, V2I, V2B, V2S, V2P |
| 4G/LTE | 450 MHz-4.99 GHz | ~100 MHz | 5 Km-50 Km | ~ 1 Gbps | • High data rate<br>• Large coverage range<br>• support nodes mobility | • Require additional network infrastructure<br>• Network capacity issue<br>• Costly | V2V, V2I, I2I, V2U, V2P, V2C |
| WiMAX | 2.3-2.4 GHz, 2.5-2.7 GHz, and 3.4-3.6 GHz | Adjustable 1.25 M to 20 MHz | 5 Km-50 Km | ~ 100 Mbps | • Moderate data rate<br>• Higher coverage range<br>• Higher mobility support | • require an additional network infrastructure<br>• It is a significantly power-intensive technology<br>• Costly | V2I, I2I, V2C, V2U |
| mmWave | 30-300 GHz | .. | ~1 Km | ~ 7 Gbps | • Extremely high data rate<br>• acceptable coverage range<br>• Good mobility support | • Limited Range<br>• High penetration loss<br>• Limited diffraction<br>• LoS requirements | V2V, V2I, I2I, V2B, V2S, V2P, V2C |
| 5G | 600 MHz-300 GHz | .. | Up to several Km | 1-10 Gbps | • Extremely high data rate<br>• Large coverage range<br>• Higher mobility support<br>• Supply further features: ProSe, edge computing, and Network Slicing | • Require additional network infrastructure<br>• Network capacity issue<br>• More costs for deployment | V2V, V2I, I2I, V2P, V2C |
| Bluetooth | 2.4 – 2.4835 GHz | 83.5 MHz | ~200 m | 2 Mbps | • Minimum cost<br>• Low power consumption | • Short-range<br>• Low data Rate | V2V, V2I, V2B, V2S, V2P |
| Zigbee | 2.4 GHz | 915 MHz (US) and 868 MHz (Europe) | ~70 m | 250 Kbps | • Very low cost<br>• Low power consumption<br>• Costly | • Short-range<br>• Low data Rate | V2V, V2I, V2B, V2S |
| Satellite | L-band (1-2 GHz), C-band (14-8 GHz), X-band (8-12 GHz), Ku-band (12-18 GHz), Ka-band (26-40 GHz), | 90 MHz | 1000's km | 10 Mbps (UL), 1 Gbps (DL) | • Extensive coverage<br>• More scalability | • High latency<br>• Burst error issues<br>• Require installation of Large antennas<br>• LoS requirements | V2V, V2I, I2I, V2U |

vehicles with direct V2V connections to exchange their status data to avoid collisions or forward these data directly to RSUs to give the vehicles prior warnings messages to take appropriate actions [101]. These messages may contain intersection-related information such as traffic signal status and scheduling, traffic density, road priority, and current weather status [102], [103]. As a result, human life will save and roads accidents are minimized. Also, through roadside sensors and cameras, RSUs can give alerts packets to vehicles when they know of any breaches, such as if the driver continues moving even when the traffic signal is red [104] if the driver exceeds the allowed are to stop in the intersection when the stop sign is active [105], [106] and to alert the driver to move when the traffic signal goes to green light [107].

Many reaearch works have beed suggested models for saving pedestrians crossing through road intersections, in [108], the authors suggested using sensors installed in intersections to collect data about pedestrians crossing the intersection. A warning message will be broadcasted to all vehicles approaching the crosswalk region to inform the vehicles that some pedestrians can avoid the accidents.

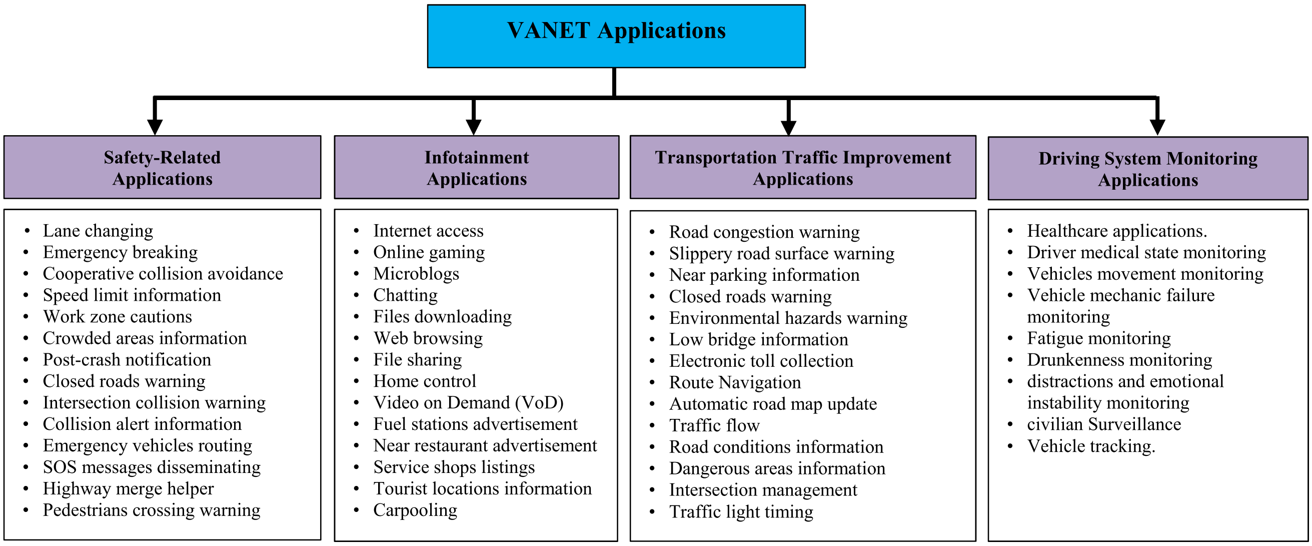



**FIGURE 8.** VANET applications classification.

For more comprehensive, VANET provides public safety-related applications that are considered to enhance the safety of drivers and pedestrians. For instance, this application can provide emergency vehicles with the optimal route to access the accident area with minimum delay. VANET can reduce the traffic density towards the accident area by providing the vehicles with the emergency vehicle's path, velocity, direction, and accident area location [109].

Another application is intended for public safety in case of natural disasters that may cause direct danger to human life through disseminating SOS (Save your Souls) messages that may include significant data such as location, voice records, and images for early aid [102]. Also, on the highway or in remote areas, VANET can help send post-violation alerts messages to inform the approaching vehicles about the stopped vehicle due to mechanical failure, collisions, or weather status to decrease the possibility of collisions or collisions traffic jams [110].

Away from that, some warning messages should inform the drivers to be aware of the dangers when approaching specific areas such as schools, animal crossing zones, road preparing zones, and hospital locations. Using the received messages, the driver can change the route or decrease the vehicle's speed to avoid potential crashes [110]. Also, vehicles should share positions, velocities, and directions to minimize the probability of rear-end collisions. For example, an alert message should be disseminated instantiously to inform the vehicles about the sudden braking made by prior vehicles [109].

This is particularly valuable when the driver's visibility is restricted because of weather status or vision is blocked by around vehicles [111], [112]. The sudden lanes change is another example of safety-related services. In this case, when the driver operates a lane change signal, and if they go towards this hazardous lane, it will caution the driver about that situation [110].

Also, the highway merge helper system aims to prevent crashes if the driver wants to merge on highways. It transmits a warning message to inform the vehicle about other vehicles' location, speed, and direction to evade crashes during the merge attempt [113]. Such systems may be built-in vehicles controllers but also requires more information from the surrounding environment [111].

### B. INFOTAINMENT APPLICATIONS

The infotainment or non-safety-related applications provide entertainment to drivers and travelers during a trip, such as online video sharing, online gaming, Internet services access, VoIP, and more [114], [115]. These applications may require high bandwidths and can put up with some delay [116], [117]. However, this type of application can further include three categories: entertainment applications, online e-commerce, and city announcement applications.

The travelers can use VANET Internet connectivity if the other known Internet access networks (Wi-Fi, Wi-MAX, etc.) aren't accessible. Even with such networks, a vehicle linked to the Internet using these networks can provide other vehicles with Internet access through VANET [118], [119]. Peer-to-peer applications that can benefit VANETs, such as gaming, chatting, file sharing, and IPTV are good examples of these applications [120], [121].

On the other hand, numerous companies utilize VANET to declare their services and goods through broadcasting advertisements messages through VANET infrastructure in their zones; for example, petrol fuel stations can declare their prices or roadside restaurants can announce their menus to appeal to travelers. Alongside this, some VANET applications help travelers search nearby shops or markets, etc. [106] [122]. Also, the nearest parking navigation applications can be used for navigating the unused vehicles space during peak times [123].

For more attractiveness and comfort, VANET allows broadcasting tourism information about the nearest tourism locations and its services through V2V multi-hop communication [124], [125]. Besides this, carpooling or car-sharing services can allow travelers to search for others who intend to go to the same destination to share the vehicle among travelers. This facility can be used to optimize the transportation system and decrease the cost and pollution generated through using multiple vehicles [126], [127].

### C. TRANSPORTATION TRAFFIC IMPROVEMENT APPLICATIONS

Traffic improvement applications are designed to optimize roads traffic and decrease road accidents by adjusting the traffic flow and controlling the transportation congestion. Vehicles are provided with information about traffic state. Drivers might select an alternative route if there is an opportunity for congestion avoidance to reduce the trip time [128].

However, transportation traffic improvement applications can be classified into three main categories that include intersection management, traffic congestion management, and roads status and transportation information applications.

As it is known, the most crowded places in the transport are road intersections, and any dispersion or lack of attention is possible to cause a crash [129]. Traffic signals operate at a specific time and do not consider the presence or density of vehicles on a particular road compared to others. For optimal results, adaptive traffic light timing can be the prestigious solution to adjust the traffic of a specific intersection by using the current statistics of traffic density on the road of that intersection [130]. Moreover, machine learning algorithms to provide intelligent traffic lights can ensure more efficient intersections management [131], [132].

Road congestion management applications are designed to keep up good traffic flow by using roads traffic status to reduce road congestion. Consequently, this will improve the transportation system and avoid traffic congestion [133]. VANET will report warning messages to vehicles around the roads in the congested state to notify the drivers about the road status and provide them with the best possible routes to their destinations [134].

One of the other applications that aim to reduce vehicle stoppage and congestion is an electronic toll collection application that allows the road tolls payment process to be achieved electronically without the stop of vehicles in the toll collection sections [123]. Also, digital maps can be one of the traffic congestion avoidance tools that can support the drivers with the correct route to their destinations without driving the wrong way. Digital maps of particular areas can be downloaded by the drivers to be used as a trip guide before moving to a new region [133].

However, some information is necessary for public transportation optimization and can also be helpful to drivers to find alternative routes. Weather status, slippery roads (e.g. ice or oils), closed roads, bridges altitudes, temporary lane changes, and human collection such as bazaar, National celebrations, or peaceful protests are good examples of information broadcast to vehicles to vehicles optimize the whole traffic system [135].

### D. DRIVING SYSTEM MONITORING APPLICATIONS

These applications are concerned with monitoring the driver's health condition while driving and monitoring vehicle status and its various parts. These applications can be divided into several categories: healthcare applications, driver physiological behavior monitoring applications, vehicle moving monitoring applications, and vehicles mechanic monitoring applications.

Healthcare applications can monitor the health status of drivers and provide the collected data to the nearest hospitals or medical professionals. Some drivers may suffer from chronic diseases or some treatments that may cause fainting or loss of consciousness, which may cause loss of control of the vehicle and the occurrence of accidents [136]. Driver's health monitoring achieves through a wireless body sensor network (WBSN) consisting of abnormal measurements. The driver would be informed, and the early assistance message would be broadcasted through the vehicle's OBU to nearby clinics or medical centers [137].

The physiological status of the driver is critical for public transportation safety. Fatigue, drunkenness, distractions, and emotional instability decline the driver's reactions and possibly cause the vehicle to be out of control and cause a transportation disaster. However, the system of detecting the drowsy driver or the distracted driver can improve traffic safety by monitoring the driver's state and triggering an alarm tone to inform the driver as soon as a drowsy or severe distraction state occurs. Moreover, the VANET warning message can be broadcasted to all the nearest vehicles to avoid the crash [138].

Also, another application in such category that is can be used to notify and provide a warning to drivers under alcohol to prevent vehicle accidents. The warning message should be broadcasted to the nearest security office to take appropriate action [139]. Also, the drivers who are suffering from emotional state disorders may increase the possibility of road traffic accidents so the integration of WSN and VANET can provide an excellent solution to monitor drivers' emotional states to avoid such types of accidents [138].

Moreover, monitoring a vehicle's mechanical system, such as the braking or steering system, can significantly reduce the damage resulting from sudden failure in those systems that may result in the loss of control of the vehicle and cause fatal accidents and collisions. However, WSN can monitor the vehicle's moving and mechanical parts and then inform the driver about any failure. Also, the VANET can notify the driver of the nearest maintenance centers and transmit the failure message to the city board or cloud to make an appropriate decision [140], [141].

The community security concerns such as tracking stolen vehicles or locating vehicles owned by criminals can be fixed through VANET infrastructures. Using a vehicle's OBU ID,

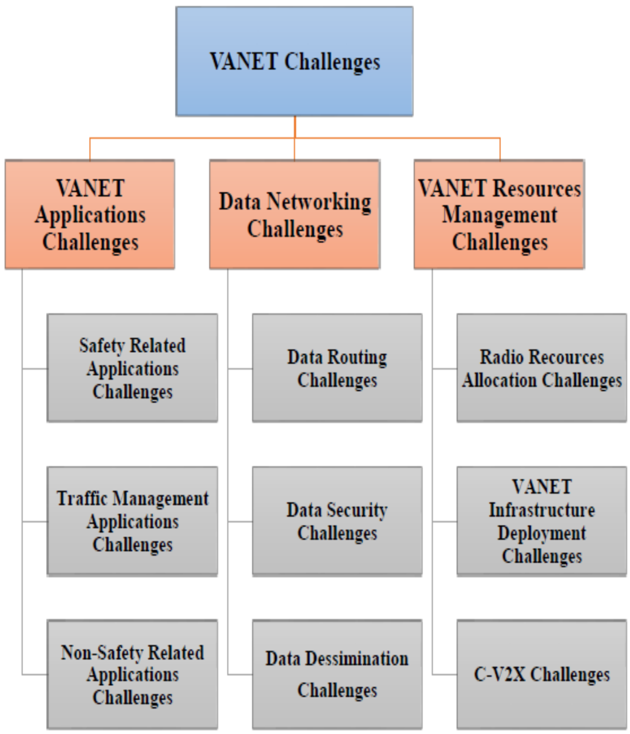



**FIGURE 9.** VANET challenges taxonomy.

surveillance cameras, and GPS information, VANETs can help the police officers quickly determine the intended vehicles' current location.

VANET would use the vehicle's OBU ID that is provided when the vehicle associates with VANET to use to track where an intended vehicle has been located [142]. Using VANET based tracking system can reduce the time required to localize the vehicles, such as it is updatable even with vehicles movement [143]. However, self-driving or autonomous vehicles, as expected, will take the lead in the world of automobiles and transportation. So the VANET necessity here will increase and witness the emergence of different services and applications to serve these vehicles and save nearby people and mitigate accidents.

On the other hand, smart cities infrastructures are in continuous development and such development may result in the introduction of new VANET related services and applications. Such applications need more attention to be realized in different VANET scenarios. Moreover, many networking and computational requirements will be necessary to deploy these services in real-time environments.

However, different VANET services will have various challenges and issues that need to be examined carefully before real-time deployment. The next sections will introduce the challenges for each services category.

## VI. VANET CHALLENGES

VANET can be suffered from different challenges that cause high limitations and restrictions on its deployment. As shown in Fig. 9, VANET challenges are classified according to VANET applications, data networking, and VANET resources management. This classification can help the researchers and developers determine what is required to be improved and where they can improve it.

### A. VANET APPLICATIONS CHALLENGES

One of the most popular aims of VANET is to deliver proactive warning messages with timely responses and high reliability to ensure safe travel. However, the applicability and deployment of VANET services and applications face many challenges that differ with the type of service and its requirement [8].

#### 1) SAFETY APPLICATIONS CHALLENGES

1) Low Latency Requirements: along with warning messages, safety applications, for example, are frequently utilized for lane change management and providing automatic emergency breaks to avoid collisions [24] . These applications should be delivered with minimum time for reaction response. However, many factors make timely decisions a big challenge in the VANET environment. Many inherited reasons cause to increase in the reaction delay, such as data processing, data security, bandwidth channels competition, routing discovery, and failure recovery. Latency is considered an essential aspect of vehicular communication. It is mainly dependent upon the optimization of the resources. In this regard, cloud computing technologies are gaining popularity due to their increased efficiency. However, the cost of cloud services in VANET becomes prohibitively expensive when the number of vehicles increases exponentially. The increase in costs is due to many operations such as sending user information to the cloud database, storing user information about channel state information, computing load in the cloud, quality of service needs, vehicle tracking, and providing customers with efficient resources access. All of them add latency to the network. To improve the latency requirements, MEC can be used for caching services at the edge of the network [144]. MEC introduces great benefit to vehicular communication through minimizing latency and backhaul bandwidth consumption. MEC brings the computation and storage capabilities near the network edge (e.g. vehicles) where the actual data is produced, attempting to avoid the delay generated from the access and use the centralized cloud systems. MEC supports data flow acceleration and real-time data processing, with low latency. Also, it can provide real-time vehicular data, such as real-time network load and localization information [144]. Accordingly, the overall latency will be reduced and the delivery rate will be enhanced. MEC allows to utilize the nearby devices such as cellular infrastructure to process vehicular data and make decisions in a near real-time manner so as to eliminate the delay. Likewise, MEC can

minimize the delay generated from offloading tasks to the cloud through caching the content on the way from cloud to end-users. Besides, it minimizes the use of backhaul bandwidth considerably since it can process and deliver large amounts of data near the vehicular nodes. By using MEC, the safety-related applications can provide without increased latency and high costs backhaul links. MEC and content caching possibly will maximize VANET capacity through caching popular content to the edge nodes and RSUs, and by improving the backhaul bandwidth. Recently, 5G-SDN-MEC framework can optimize VANET latency by providing a URLLC facility [145].

2) Communication Scalability: VANET connectivity is mainly dependent on the vehicles that go from the road. The requirement for the data transmission relays (i.e., vehicles, RSUs, BSs) increases when vehicles decrease. In these instances, connectivity must be maintained at a high level where the network can scale up or down flexibly in response to the increased number of vehicles and other significant circumstances. The utilization of supportive infrastructure such as UAVs to be used as data relays when the distribution of the vehicles is low can enhance the network connectivity. Also, the availability of vehicles is unstable, so using traffic-aware model to determine the supportive infrastructures is a good solution here [17].

3) Scheduling: Scheduling becomes more complex in vehicular networks because connections in VANETs can be irregular. However, the increasing number of vehicles can cause a massive flow of packets into RSUs. This large number of packets will lead to an overload on the RSU computation and storage units, causing a high delay in the data arrival and response rate [26], [146]. Therefore, how to address this defect by resource management and data scheduling according to its significance and giving priority to the most critical data or to those vehicles that have an unstable transmission line can contribute to providing better solutions. Also, efficient buffer management and packet scheduling schemes such as distinct queues for different outgoing links or services can help improve resource management and packets scheduling.

4) Critical Data Validity: In VANET, safety-related data should be delivered using V2V or V2I communications within a minimum time in some specific area. However, the vehicles' information such as mobility, GPS position, and direction should be frequently updated to be used in many safety-related applications to prevent possible risks or traffic congestion. This problem remains a concern in the vehicular network, where data should be analyzed and fused efficiently. When transportation agencies request real-time traffic information, it is impossible to transmit all of it. Thus, updating and eliminating outdated data helps to improve resource consumption and the reliability of the delivered service [147]. Designing strategies for validating and providing data to give users the essential helpful information on-demand is necessary. Using context information such as vehicular traffic density, mobility pattern, and vehicles distribution with ML algorithms can help predict the usability and validity of critical safety-related data. Also, integrating other data analysis and fusion technologies, such as fog and edge computing can provide highly reliable results.

5) Network Resources Scarcity: Many wireless and communication technologies facilitate data transmission in vehicular networks. Nevertheless, the scarcity of frequency channels and bad connectivity is still a significant challenge. As a result, sufficient bandwidth channels are necessary to realize safety-related applications. Some communication systems can support safety-related applications by offering additional resources. For example, the 5G paradigm [84] is an encouraging solution that has the ability to mitigate this deficiency. Also, using cognitive radios and VANET as another solution to overcome the bandwidth scarcity in VANET can help provide the required channels for safety-related packets transmission [10]. However, many challenges face the utilization of other networks resources in VANET applications, such as data security and privacy, resources compatibility, usage billing, and others [12].

6) Safety-related data inconsistency: Recent years have seen a significant proliferation of innovative technology and equipment in the automotive industry. As a result, various vehicle models have different computation power, storage, and Internet connectivity [19]. As a result, incompatibility and inconsistency occur, and interaction between vehicles may fail. So handling such heterogeneous nodes is a big challenge in providing time-sensitive safety-related applications. For example, some proactive safety applications require accurate location information to be exchanged with the RSU. Yet, due to the presence of multiple GPS versions, the RSU will collect position information with variable degrees of precision [148]. Several safety-critical applications have restrictions in global positioning systems, particularly where sub-meter reliability is required, and these restrictions are dependent on the localization accuracy level. As a result, various efforts must be made to deal with interoperability. Thus, to address the issue of interoperability among heterogeneous network nodes, standardization can be employed to achieve agreement among the stakeholders (i.e., car manufacturers, developers, etc.) engaging in VANET [149].

7) High Vehicles Dynamism: The increased mobility of vehicles can cause extreme dynamism in the VANETs topology. The vehicles move in unpredictable patterns and at very high speed, so it may have insignificant time to associate with nearby vehicles. This

issue leads to a high possibility of to lack the vehicle inter-communication. The high vehicles mobility will increase the degree of disconnectivity, resulting in a high delay in delivering safety and caution messages [20]. Thus, the connection time must be considered [3]. This high degree of dynamic behavior creates a bottleneck in traffic control and driving safety. Also, the collaboration between VANET members and traffic authorities has a high impact on enhancing safety services such as collision avoidance, work zone alert, and closed roads cautions. Vehicles can gather, process, and share data via their sensors. Additionally, the data might be sent to traffic authorities to make decisions and report them to vehicles [150]. Discovery procedures begin when a communication link fails, resulting in higher packet delivery delay, data leakage, and network congestion due to the additional control messages. ML models can make a suitable decision for vehicle mobility estimation and context information.

8) Multi-sensors Relevant Data Synchronization: The vehicle's data may come from various sources: its sensors, those of other vehicles, the RSU, and perhaps social networks. One significant problem in managing multiple data sources is its synchronicity. For future applications, safety-related decisions should be made according to the cooperation of various sensors. For instance, in autonomous vehicles' 3D object detection system, the camera capturing and point cloud should be used simultaneously, so the storage system must synchronize prior use or share it with other vehicles [151]. The synchronization process may cause to increase in the delay of safety-related applications. This problem becomes more complicated when the accuracy of timestamps from multiple sensors varies. ML-based systems can be developed to cooperatively fuse the data produced from different sensors for high-quality results.
9) Failure Detection and Diagnostics. Now, the vehicles depend on the embedded sensors for the detection of the road status (e.g., accidents, obstacles, and pedestrians) and severe environment changes (e.g., road stumbles, heavy rain, and heavy snowfall. Though we can leverage embedded sensors to provide a complete picture of the surrounding area, several outstanding issues regarding failure detection remain. Even when sensors operate correctly in a real-world application, the collected data may not accurately reflect the actual situation and provide incorrect information to drivers [152]. For example, the camera may be blocked by unexpected obstacles like leaves or dirt, or the radar may shift from its initial static position because of the wind's effect. In this situation, detecting sensor data failures is extremely difficult. Many safety-related services use the sensor data for decision-making. Vehicles can acquire different information such as their position and direction using embedded sensors [19]. Unfortunately, the failed and wrong detection can be shared with other vehicles, resulting in high unreliability in the critical safety-related services.
10) Weather effect: VANET deployment may be affected by extreme environmental conditions like heavy rains, high winds, and snowfall. However, these conditions will affect the sensor's detection and degrade the radio signal propagation, causing weakness in control signals received from RSUs. However, developing a mechanical system with a high ability to cope with these conditions and enhance V2V communication is a big challenge.
11) Data Security and Privacy: One of the most significant challenges facing the dissemination and exchange of safety-related data is its security, privacy, and authenticity. Any wrong change or modification in the shared information within the VANET network may cause more traffic jams or fatal accidents. Also, it is possible that the hacker impersonates another vehicle and sends the wrong messages to the RSU. More than that, he can change the correct data and resend it by participating in the multi-hop V2V communication. Moreover, the robust data encryption algorithms require a high computation load, increasing the consumed energy and data exchange latency [23]. However, focusing on the confidentiality of critical data more than others can cause an imbalance in the protection of the network, so it has become necessary to search for new algorithms to compromise the security of critical data, taking into account the importance of other data.
12) Multiple Data Input: Many safety-related applications require a collection of input data to make an optimal action. For example, crash avoidance requires several considerations that must be maintained when deciding on an alternative action, such as traffic signals, pedestrians, guidance instructions from the nearly RSUs, and other vehicles' perceptions [153], [154]. In the worst-case scenario, this makes it more difficult for a driver to concentrate on all of these consider-ations concurrently. As a result, investigating multiple data aggregation becomes critical in this situation.

#### 2) CHALLENGES OF TRAFFIC MANAGEMENT APPLICATIONS

1) Infrastructure Deployment Costs: The fundamental goal of traffic control and management is to optimize road traffic, minimize journey times by avoiding traffic congestion, and help drivers by updating existing traffic conditions and recommending alternative routes [21]. This may demand the deployment of specific roadside devices, such as intelligent traffic signals and electronic signboards, which can be controlled using ML algorithms. [24]. Also, the deployment of assistants such as UAVs can improve traffic density estimation. Nevertheless, it will bring many challenges, including costs, management, mobility, and privacy concerns [16], [17].

2) Computational complexity: Traffic management applications deal with big data generated from roadside units, pedestrians, vehicles, cloud servers, and so on [22]. This data, to be beneficial, should be analyzed to make optimal traffic management-related decisions. The development of efficient solutions to minimize the computational complexity and have the ability to help in predicting the density of road traffic is a big problem in the deployment of traffic management applications.
3) Prediction Accuracy: Awareness of potential traffic problems can aid in the alleviation of congestion and the expansion of road capacity. Traffic flows prediction is vital to minimize traffic congestion [53]. Predicting vehicles' mobility and their density over time are essential factors in VANET data transmission and routing [32]. However, the non-uniform vehicles distribution and high mobility result in a significant challenge in the vehicular predication solutions [3]. Awareness of weather and traffic conditions seems critical to optimizing traffic management applications that require more research attention.
4) Packets Storm Problems: Road congestion management applications, are designed to keep up acceptable traffic flow through roads traffic status to reduce road congestion. Consequently, this will improve the transportation system and avoid traffic congestion [155]. VANET will report warning messages to vehicles around the roads that are in a congested state to notify the drivers about the road status and provide them with the best possible routes to their destinations. This will generate a considerable number of warning messages that may travel through the network, causing network congestion and QoS degradation.
5) Sensors Data Accuracy: However, some of the necessary information for public transportation optimization can be acquired through onboard vehicles sensors. Weather status, slippery roads (e.g., ice or oils), bridges altitudes, and human collection such as bazaar, National celebrations, or peaceful protests are good examples of information generated using onboard sensors and embedded acquisition systems [135]. Transportation agencies will depend on the data to make further decisions. However, any failure in the sensing process may generate fault decisions. As a worse case, when this data is broadcasted in the VANET network will cause to disseminate erroneous information that causes a high degree of unreliability and system untrustworthiness.
6) Security: Traffic improvement applications are designed to optimize roads traffic and decrease road accidents by adjusting the traffic flow and controlling transportation congestion. Vehicles are provided with information about traffic state. As a result, drivers might select an alternative route if there is an opportunity for congestion avoidance and reduce the trip time. The security of these data is vital where its attack may cause high congestion, transportation errors, and wrong routes following. The hackers can pretend to be legal participants and provide transportation agencies with fault information that can affect the whole transportation system. Therefore, the security and authentication of traffic improvement information should have more attention. Besides, security of VANET is a vital concern and should be considered in a systematic and holistic method. In this regard, the adoption of security-by-design principle for VANET security can bring high security benefits. However, security-by-design principle can be utilized to generating security monitoring and optimization platform that includes mechanisms for evaluating and improving the security of VANET applications, during their overall development lifecycle, and particularly during the requirements, design, coding, and testing phases [69]. Accordingly, security-by-design principle helps the developers of VANET-based applications to determine the security requirements uniformly and concretely during the design and requirement phases, make sure the adherence of the created VANET application to the originally determined requirements, detect potential vulnerabilities and assess the security level of the real-time VANET application, and introduce recommendations for overall security improvements. In that way, such security platform can offer a more holistic security assessment, as it covers all the phases of the development lifecycle of VANET applications horizontally [69]. In general, the use of security-by-design principle in the security of VANET applications is still in its infancy and requires a lot of research work to develop and improve.

#### 3) INFOTAINMENT APPLICATIONS CHALLENGES

1) Security: drivers and travelers can benefit from infotainment applications such as marketing, parking availability, and highway tolling. However, it is essential to exchange and share legitimate copies of such data without modification or misuse. The hacker can broadcast false information and advertisements, which is confusing when using that data. Also, he can attack the forwarded data through multi-hop communication and reveal incorrect network information [1] . One of the main challenges in the security of infotainment data is its vast data size. This will require more computation processing and high latency to secure the actual data [44]. Hence, verifying security services for infotainment services is a big challenge.
2) Unfairness: Most of the algorithms and solutions suggested for routing and exchanging data in the VANET networks mainly focus on safety-related and public transportation management services, so infotainment services have been taken less attention. This neglect concentrated primarily on the reservation and exploitation of network resources for safety-related services,

which led to a decrease in the QoS and QoE of the entertainment services [2]. However, developing networking algorithms that can ensure fairness in resource utilization by both safety and non-safety data transmission is a big challenge.

3) Bandwidth Requirements: Many infotainment services, such as videos on-demand, online games, or video conferences, require high transfer rates to ensure services reliability and continuity—however, high frequencies are needed for providing acceptable data transfer rates for these services [156]. The DCRC/WAVE does not provide sufficient bandwidth to ensure the high throughput requirements for infotainment applications. This deficiency may lead to many problems in providing these services to the consumers [76]. VANET communication can be improved by utilizing the high advantages of cellular networks with conventional and upcoming applications of VANET [157]. The use of 4G/LTE and 5G cellular networks for VANET communication has recently grown in popularity [158]. Cellular networks can provide wide coverage area and supports bandwidth applications demanding higher data rates [158]. Many simulations based studies shown the efficiency of cellular networks including 4G/LTE and 5G systems in multimedia data transmission in terms of latency, packet delivery rate, and throughput [157], [159], [118], [160]. They have proved the latency and message delivery ratio of cellular based VANET communications outperform that of the DSRC based VANET. Moreover, due to high bandwidth of cellular communications, the computed throughput demonstrated the performance of cellular communication with VANET bandwidth-hungry applications. Still, the security, handover management complexity, subscription fees, and competition with the users of such systems are the main challenges in this paradigm [80], [121]. On the other side, the using of high frequencies such as mmWave and THz bands can enhance the transmission rates required for bandwidth-consuming services [80]. Unfortunately, these techniques include more challenges that should be investigated, such as beam alignment, blockage detection, and short wavelength [82], [161].
4) Different QoS requirements. Advances in VANET networks enable a variety of deployment architectures for VANETs on highways, in urban and rural areas, to meet a wide variety of infotainment services with varying QoS needs. Typically, various VANET applications demand different levels of QoS. For example, real-time applications (such as voice conferencing) are frequently time-sensitive. Thus, packets must be sent within a specific time frame with a minimum packet loss, but they may tolerate occasional bit mistakes. In comparison, data-hungry services such as file sharing and video on demand are typically less sensitive to delays but require more data accuracy [26]. Following that, we need solutions to differentiate the QoS requirements of each infotainment application. The diversity of such applications results in more difficulties in constructing a single model with a set of predefined parameters for evaluating QoS for each application. Additionally, the data type sent is a significant element in determining the system's performance. Therefore, the process of balancing the networking matrices that achieve the required QoS according to the type of service provided may be one of the problems that require deep research.
5) Comprehensive QoE Modelling: The QoE concept has been commonly applied to describe user perception. Several models and tools for evaluating network services have been developed concerning QoE modeling, measurement, and management, with the examination of numerous contributing aspects. In the QoE monitoring, we measure or estimate the QoE of delivered services using dedicated tools with the consideration of the influencing factors. In QoE modeling, models are built to measure or evaluate the QoE in a manner that is as similar to the QoE received from end-users as possible [25]. However, the dependency on the feedback from customers includes many challenges such as communication overhead, unrealistic results due to the user's urgency or negligence in filling in the feedback form, and users' annoyance. Therefore, it has become necessary to develop automated solutions based on AI techniques to deduce influencing factors on the QoE and predict the extent of users' satisfaction with the services provided without the need for feedback from the users themselves [162]. The central concern in the quality predictor systems is the selection of relevant influencing factors to estimate the QoE for several infotainment services in various environments and situations. There has been no standardization of QoE influencing factors, measuring methodologies, or prediction of QoE in the research of VANETs environment. As a result, it is critical to conduct research to standardize the QoE across VANET for various information and entertainment services.
6) Data Analysis and Storage: Many of the non-safety services delivered in the VANET generate vast volumes of data, such as video conferences and online games. The processing of such massive data may be challenging and requires high-quality embedded hardware. On the other hand, these data will require large storage units for caching or storing them. As a result, these challenges can cause the emergence of many problems that may affect the acceptability of the services for users. However, developing efficient systems for image/video data processing capable of outputting images with high resolution to the driver is a significant problem. For such applications, it is valuable to accomplish data compression algorithms [163]. ML-based multimedia data encoding should be developed to provide high

results in the VANET data representations and consequent reconstruction. In this regard, the huge amount of data generated from infotainment services requires the coordination of computing resources and flexible network management. MEC as a new network paradigm can be utilized here to provide resource management and services at the edge of VANET network and, so, nearby the vehicles ensuring low latency and high bandwidth requirements [87]. MEC can offer efficient solutions to infotainment data storage and analysis through providing computing resources, storage capacity, connectivity, content retrieval, services caching, and network information for requesting vehicles [145]. MEC can host infotainment services and applications closer to vehicles decreasing the issues of infotainment big data storage and analysis. For instance, only the data acquisition part is processed at the vehicle, while other processing parts can be offloaded to MEC servers. Recently, the concept of MEC-enabled RSU have been introduced widely [141], [144]. Hence, by caching contents before delivering them to the vehicles passing by, RSUs can play as agents for information dissemination without fetching from backhauls. However, such incorporation is a challenging matter. The interworking between MEC servers and RSUs has not been studied in detail yet. Also, services priority, energy efficiency, on-demand scalability, and multiple-MEC management represent a development challenges that are still required more research attention.

7) Devices Incompatibility: Infotainment services include many applications that generate and exchange data in the forms of image, audio, or video data. Requesting access to one of these applications may require display devices embedded in the vehicles or handheld devices of the driver or passengers. In any case, the embedded display devices can come with different characteristics from one vehicle to another, such as screen dimensions, display resolution, or data encoding causing many problems in data representation and display. As a result, the lacking of standardization may lead to many issues of devices compatibility.

### B. DATA NETWORKING CHALLENGES

VANET communication is based mainly on Inter-Vehicle Communications (IVC) to allow vehicles to form mobile communication networks and share their data, enabling ITS to provide various services without depending on centralized communication systems. Here, the main challenges that face data networking in vehicular communication will be introduced from three main aspects that are data routing, data security, and message dissemination.

#### 1) DATA ROUTING CHALLENGES

Routing in a VANET is a difficult task. Identifying the shortest path that satisfies latency constraints and has the least possible overhead is fraught with various restrictions and challenges. These challenges arise due to vehicles' high mobility, frequent path breakdowns, and numerous blockages, all of which can impair the reliability of data delivery and routing. However, the main challenges that face the success of data routing in vehicular communication can be listed below.

1) Traffic awareness: Traffic awareness refers to a protocol's ability to utilize traffic conditions to choose the most efficient route. Traffic information such as vehicles' kinematic information such as locations, velocities, and directions can help determine the traffic information at a specific period. However, the routing protocols need continuous real-time measurements to choose flow disruption and find the best routing paths. This will cause high communication overhead through broadcasting the vehicle's kinematic-related packets at periodic times. However, there are a large number of studies to estimate and predict the traffic density [28], [164], [165], but neither of them discusses how to obtain real-time traffic data. [27]. Moreover, the high mobility and random distribution of vehicles may lead to erroneous estimations for vehicular density. As a result, any solution regarding vehicle traffic volume without real-time implementation is incorrect, resulting in illegal routing protocols. [27].
2) Lack of required information: in a dynamic environment such as VANET networks, it is necessary to utilize many factors such as link stability, blockage detection, and nodes mobility to determine the optimal paths toward the final destination. The packet should include additional information about the complete route from source to destination. Unfortunately, the high mobility of vehicles will result in many changes in the route information encapsulated in packets resulting in either packet with increased size, especially if the number of intermediate nodes is a significant or high number of lost packets [166], [167]. As a result, using several forwarding metrics as an alternative to a single metric can improve the routing process. Still, at the same time, it will bring more challenges that are required to be investigated.
3) Network connectivity: VANET networks distinguish by many issues that make communication reliability and continuity a big challenge for every routing protocol. Vehicles can move with high mobility at random intervals. Many of the suggested routing protocols are based on ML techniques for predicting vehicles mobility. The dependency on the vehicle's mobility prediction can reduce the latency of routing discovery [55]. However, none of them used online training or can provide real-time prediction [28], [134]. Moreover, on the highway or urban roads at specific periods (e.g. holidays, nighttime), network connectivity may be low due to the number of the vehicles being small or insufficient to deploy routing protocol [57].

In a VANET, there is a trade-off between optimal traffic volume and connection; hence, a sparse location gets weak connectivity, but a dense region may have congestion, resulting in packet loss or latency. In dense areas, the likelihood of certain vehicles being placed near the border is greater than in sparse ones. As a result, traffic density can be used to optimize forwarding behavior. Priority should be given to packet forwarding via vehicles closer to the border in a dense region over vehicles closer to the source; in sparse environments, density has no influence. The multiple disconnections make the application of any routing protocol in the real-time environment in a big suspension. Vehicle dynamics will be significantly altered by variations in their individual routes and activities. The movement is generated over time by variations in the driver's target location. As a result, the development of new algorithms for predicting driver perceptions may result in more accurate forecasts of successful results. So, alternative methods such as UAV relays in the disconnectivity area can deal with the subsequent network disconnection.

1) Next-hop selection: When the routing protocol is based on selecting the next-hop by the intermediate relay node, the link recovery packets will not be required to be directed back to the source vehicle when the link fails. As a result, the source will not know when the message is not delivered. Otherwise, full path selection will not be a highly reliable solution in a VANET environment where the numerous disconnection would increase the flow of the control packets, increasing network congestion. However, for best results, the selection of the next-hop relay should utilize more factors in determining the next-hop node, such as vehicles mobility, blockage effect, link stability, path lifetime, vehicle destination, and so on [167], [168], [169], [170]. Even though vehicles' mobility is limited to roads, it is supposed that vehicles are distributed randomly and freely regarding velocity and direction. Vehicles operating inside the same wireless communication area can be pushed out of range due to the velocity differential and spaces separating them. To guarantee that the communication between two vehicles remains stable, the communication range must be maintained. The average motion of the sender vehicle and its neighboring vehicles should be taken into account while selecting the next hop to reduce the incidence of link breakage. This can improve the VANET's QoS metrics. Thus, vehicles motion can play a critical role in developing a forwarding mechanism that minimizes link failures and improves link stability throughout high-mobility VANETs.
2) Radio channel model impact: The radio channel model is an essential feature of wireless communications, particularly VANETs communication because vehicles often have an antenna with low height, frequent mobility, and time-sensitive require-ments [171]. To our knowledge, most routing algorithm studies have ignored or minimized the impact of radio modeling primarily when establishing the communication range. To this end, various research studies have considered that the radio transmission range is fixed and especially impacted by signal propagation [172].

Also, radio signal transmission in vehicular networks can be hindered by obstructions like buildings, buses, and trees, among others. They may cause blocking, attenuating, shadowing, and multi-path fading. Given the diversity of the VANET environment, the channel model must be adaptable to reflect a large variety of radio channel conditions. However, the neglect of radio channel modeling in data routing will significantly impact the packet delivery rate and increase the packet error rate.

1) Impact of geographic information on forwarding decisions: Position-based techniques are more appropriate for networks with a high degree of dynamic behavior, like VANETs [29], [56]. Vehicles can use a positioning system, such as the GPS, to gather their locations and then share them with their neighbors through broadcasting control packets. By picking the most progress nodes within the sender's radio range, the number of hops to the destination can be minimized. As a result, the end-to-end delay of packet forwarding is lowered [57]. Constructions and infrastructure are a significant cause of position inaccuracy and may degrade the GPS signal's power. Due to direct satellite invisibility, GPS accuracy ranges from around 20 meters to 30 meters; therefore, they are not suitable for urban high-density vehicular environments [173].

Even when satellite signals are available, a global positioning system cannot provide accuracy [57]. Other environmental factors affect GPS services, such as poor accessed-satellite conditions and high multipath interference. Therefore, the positioning system readings should be precise enough to make the routing decisions accurately.

1) Security considerations of routing: Many routing algorithms do not examine the security risks in the data forwarding decisions. Because of the heterogeneity of nodes that might be exploited as a relay in vehicular communication such as vehicles, personal handhelds, and nearby wireless infrastructures, possibilities of attacks, like Denial-of-Service (DoS), unauthorized access, spoofing, and the existence of a malicious node need to be addressed. Also, the high computation and overhead of security algorithms and their effect on the packets' delivery rate should be taken into account when designing secure-based routing algorithms.
2) Developing intelligent routing protocols: The routing protocols are designed intelligently, where the vehicles can adaptively select the routing path with the best results. ML algorithms are commonly used in many VANET routing fields, such as next-hop selection,

location prediction, path lifetime prediction, and cluster head selection [174], [175], [176].

However, even with the high performance of using ML algorithms in data routing, there are many challenges that may negatively affect VANET communication. ML algorithms are time-consuming algorithms and require high-performance computation units. From a VANET standpoint, information should be delivered between vehicles with minimal communication overhead and delay. Also, the applications of offline learning will never reflect the real-time VANET environment. The routing protocols with self-learning ability can be a good research area in future intelligent routing protocols.

#### 2) CHALLENGES OF DATA SECURITY IN VANET

There are numerous critical requirements for VANET security. Vehicles must respond only to packets transmitted by legitimate network members. As a result, it is essential to verify the message sender. Additionally, the receiver should conduct data consistency checks to determine if the message carries incorrect data that an authenticated member routed.

To provide non-repudiation security services, the driver shouldn't deny the forwarding of a message, and the driver's identity must be precisely determined. On the other side, the driver's personal information is critical and should not be disclosed to illegitimate participants. However, the following key challenges must be explored in-depth and effectively to develop scalable solutions for their addressing.

1) Scalability: VANETs may be used to cover a variety of safety-related and infotainments applications. With the increased number of vehicles and VANET applications, big data will generate that may be vulnerable to different attacks. Still, the deployment of these services requires scalable strategies for vehicular data security, and authentication must be developed. Scalable strategies for vehicular data security and authentication must be designed to implement these services. The majority of solutions to this problem reported in the literature are centralized [23], [30]. There have been few attempts to address these issues through decentralized methods. More research required to handle the requirements of security scalability.
2) Message Authentication: Each message sent by vehicles should include a digital signature to ensure authenticity, integrity, and nonrepudiation [30]. Message authentication requires the vehicle to employ computationally intensive techniques to verify the digital signature for each received message i. This increases the computational load on vehicles for message confirmation. So if the vehicular density is high, the computation overhead on the vehicle's OBU may become unbearable. Some researchers cooperate with message authentication to reduce the computational overhead associated with message verification in vehicles [177]. Such protocols were suggested to distribute the authent-ication burden on neighboring vehicles. Cooperative message authentication may be vulnerable to Sybil attacks, as an attacker node can create multiple Sybil nodes [23]. Also, in general, these protocols select messages based on their location. As a result, they may be vulnerable to position modification threats. GPS signals need to be more precise and accurate, as differences of even a few meters can create dangerous situations and degrade the network's performance. Also, GPS is vulnerable to a variety of Location spoofing and signal jamming attacks [148]. So, effecient methods are needed to improve the network performance against different authentication attacks.
3) Vehicle Privacy: Maintaining vehicle privacy is critical in VANETs. Otherwise, the lives of vehicle drivers and travelers may be seriously compromised. As a result, a vehicle should avoid using its actual identity in all communications. Numerous solutions are proposed to this problem. Many proposals are based on pseudonyms codes rather than the existing vehicle identifiers. This involves many pseudonyms that should be loaded into the vehicles and maintained secret [178]. Additionally, even with high requirements for privacy preservation, the transportation authorities need to track and prosecute malicious vehicles. Also, vehicles should be prevented from utilizing the same pseudonym for an extended period because the unauthorized user can link the pseudonym with the actual vehicle identifier using the path taken by the vehicles. As a result, pseudonyms must be modified on a regular basis. By using changeable pseudonyms at predefined intervals, an intruder is prevented from associating two datagrams with the same vehicle and tracking it. Thus, millions of pseudonyms must be designated for each vehicle over its journey, and a scalable technique for monitoring which vehicle has been designated which pseudonym must be designed and built [179]. Additionally, for the sake of non-tracking and privacy, an efficient method for partial pseudonym allocation, butterfly keys, and linking systems aren't yet utilized. Additionally, the use of mobile IP or modifying the IP or MAC address of vehicles to evade traceability requires more research efforts.
4) Roadside Infrastructure Accessibility: A large number of security-aware protocols presented the existence of RSUs. RSUs are primarily utilized for key management and privacy assurance [177]. RSUs, on the other hand, will not see large-scale deployment in the near future. Thus, future methods should consider scenarios in which RSUs are not widely deployed. Thanks to the advances in innovative technologies and the increasing number of vehicles, it is also critical to develop scalable and reliable VANET infrastructures that enable various technologies (e.g., DSRC, D2D, and mobile networks). Vehicles in this scenario must authenticate with units owned by other networks [23]. This is most difficult

where vehicles utilize privacy-preserving authentication while other networks do not.

5) Real-time implementation and evaluation of security protocols: Any proposed solution should be implemented and tested in a real environment to show its feasibility and applicability. This realization will offer the required updates or improvements to make the solution more reliable and efficient. Several studies have suggested metrics for assessing authentication and security procedures in VANETs. Nevertheless, these metrics fall short of meeting all demands. Metrics must be advanced and standardized; additionally, simulators and testbeds should be implemented for evaluating protocols using these metrics.
6) Trustworthiness evaluation and misbehavior detection: To ensure a safe drive, it is critical to ensure that the information exchanged between vehicles via VANET is accurate and not misleading. It is essential to trust the data collected from other vehicles. VANET's purpose of advance safe and supportive driving. This is accomplished by supporting the driver or vehicle with the necessary information that requires frequent checking and verification within the VANET. Data-centric trust and verification need to conduct additional research on the tamper-resistant systems utilized in vehicles to recognize useless accident warnings. To verify the context, a vehicle should be able to behave as an intrusion detection system by trying to compare gathered messages about the vehicle's status and environment to its own existing data. Additionally, the reactive security principle must be strengthened. Analyzing the vehicle's trust is an unsolved issue, as numerous trust models have been proposed to determine the reputation level of vehicles, and vehicles interaction is centered on the reputation level that a specific vehicle acquires [180]. however, there is a number of questions that require more attention such as: On which criteria must be based to determine whether a vehicle is trustworthy or not? Would the trust measure be reliable? Is it trustworthy as a means of disseminating critical data?
7) The revocation procedure and the management of the certificate revocation list: When a vehicle's certificate is revoked due to misbehavior on the network, the RSU revokes the vehicle's certificate to prevent it from communicating with other nodes in VANET. Generally, all VANET entities must share Certificate Revocation Lists (CRLs) to revoke certificates issued via the basic infrastructure. Additionally, the keys are immediately revoked [23]. When misbehavior is identified, how should the certificate be revoked? How should the certificate revocation list be distributed? Is there overhead associated with the distribution of CRLs? These solutions are still in their infancy, despite their importance as a significant component of network security. The infrastructure does not support CRLs. The verification and revocation of certificates take longer in the case of chain certificates. This might result in an explosive increase of CRLs, slowing down message authentication. As a result, centralized solutions are inherently not scalable. Several suggested solutions for resolving this issue allow for the decentralization of producing and managing certificates and CRLs to the RSUs. Regrettably, additional research is needed to develop super-efficient, scalable, and secrecy strategies to address this issue.
8) VANET Clustering: While group formation is a trend in VANET protocols, the logistics of delivering in intra-groups and inter-groups in a VANET are not well defined. In clustering-based protocols, the group leader serves as the central server for all nodes that join the group. Also, it is responsible for key management and fundamental communication [181]. However, the control of group partitioning and communication in jammed signals is one of the significant challenges in cluster-based protocols. Also, when the group leader departs the group, the group's key should be managed scalable, and a backup group leader must be appointed to manage keys and continue the group members' security. Moreover, the criteria used to choose the next group leader are not clarified in many previous works, especially regarding security. So, many questions need precise answers such as what if the group's next leader is a malicious vehicle? What is the role of VANET infrastructure in group security and communications? and what issues of data security/privacy arise when integrating other wireless technologies in inter-group and intra-group communication?
9) Time Constraints: The robust cryptography schemes require more computations and processing time to do their operation. Messages should be encrypted before being transmitted away. The data receiver should ensure data integrity and authenticity before using it. These operations should be achieved in a timely manner. In the case of receiving unreliable data, the receiver should take appropriate action such s informing the sender or triggering the RSU to make an additional verification to check whether there are malicious nodes in the path of data transmission or more of that if the sender is the malicious node itself. Moreover, the data integrity and authentication verification may generate more delays if the data packets accessed the destination through multi-hop communication. Each intermediate node should perform the verification process before forwarding the packet. Also, keys management will generate more delays in the data transmission process.
10) Cryptographic Keys Management: The cryptography algorithms are based on using keys for data security, integrity, and authentication verification. However, the keys should be distributed securely and on time. Based on our knowledge, no studies discuss the size of security keys and authentication delays on network reliability [30]. Due to vehicles' high mobility and dynamicity,

the preferable is to assign keys of short duration. This will cause more challenges such as key reassignment problems, communication overhead, and latency of key distribution. However, the use of short-lived keys and the communication overhead caused by keys and management and revocation are good research fields requiring further improvements. Also, many VANET services are time-aware, so the latency caused by key management and distribution should be minimized as soon as possible. So, for privacy assurance, the methods of exchanging certificates at specific times are not defined yet [23], [30]. For more reliability, the proposals for using keys without credentials require more research efforts.

11) Anti-malware and Intrusion Detection System (IDS): Intrusion detection systems are critical for identifying malicious activity on a network. it is very crucial to integrate IDS into all vehicles. But even with the high benefits of IDS in VANETs, the capability of IDS to handle harmful and erroneous information on the VANET promptly is one of the significant obstacles in the IDS-VANET integration. Also, the effect of vehicles mobility and network dynamicity should be researched more to reach high results.
12) Lack of comprehensive security protection: The VANETs communications can be logically categorized in three domains include in vehicle domain, ad hoc domain and infrastructure domain [182] . Besides, V2X communications have led to diversity systems and devices to be part in the VANET communication. However, these make the security threat vectors in vehicular communications to be multidimensional [182], [183], [184], from the vehicles up to the core infrastructure. Upcoming VANET infrastructures will incorporate multiple networking systems and data access providers and integrate new models of service delivery. The development of multiple layers' security systems is essential for data protection at all VANET levels and across vast number of interconnected systems and applied applications [182]. International Telecommunication Union Telecommunication (ITU-T) have been proposed in its security recommendation X.805 [185] the security dimensions, or what is called a security controls. The appropriate application of these security dimensions can address the whole security-related architectural systems and realize comprehensive security protection [186]. They include a set of security controls to help the interweaving of security capabilities in the complete end-to-end security solution [186]. The main security dimensions include access control, identity and authentication, data confidentiality, data integrity, and communication security. The security dimensions encompass a set of security controls to promote the interweaving of security capabilities in the overall end-to-end security solution [185]. However, a number of research have been suggested to provide various solutions of the security problems in the VANETs. But the existing solutions do not confirm all the security dimensions simultaneously. Additionally, the security of data generated from embedded sensors should be considered to prevent attackers to access the raw data and change it. Therefore, it has become very necessary to use these security dimensions to build an integrated security system to protect VANET data comprehensively.

### 3) HALLENGES OF VANET DATA DISSEMINATION

Dissemination of information between vehicles and infrastructure and between infrastructure and vehicles is more critical. Exchanging vital information among vehicles, such as safety alerts, weather updates, and traffic information, is still a challenge in VANET. Numerous researchers have developed various strategies for data dissemination [31], [187]. However, this section discusses the major issues that are related to VANET data dissemination.

1) Scalability: In situations with a high VANET density, broadcast storms may occur [187]. Many VANET remain focused on scalable data dissemination, with the goal of minimizing data redundancy. Innovative solutions need to be developed to identify traffic density in order to overcome scalability concerns with data dissemination protocols. Also, necessary investigations are required to show the effect of the deployment of an additional VANET infrastructure to help in message dissemination and cope with the scalability issues. The improvements and using context information and situational statistics of VANET resources can decrease the communication overhead caused by data dissemination protocols and increase its scalability.
2) Security and Trust: Integrating security protocols into VANETs is critical for safe data dissemination [31]. Users will not tolerate warning systems that lack confidence, security, and reliability. Establishing trust through the provision of trustworthy programs is regarded as the most critical security challenge in a VANET. So, integrating security mechanisms with data dissemination-based protocols will increase message delivery latency. As a result, mitigating the issues of security integration with dissemination protocols requires more attention.
3) Cooperation between nodes: Most VANET dissemination techniques presuppose that nodes are cooperative and willing to share their resources to enable communication with other nodes [31]. This assumption, however, is not always valid. Additionally, in heterogonous VANET, some vehicles may reflect destructive behavior, enabling other nodes to use their services while denying equivalent usage of their resources with the same nodes. Protocols and systems would need to enforce proper reward, punishment, charge, and credit mechanisms.

4) Simulation: Due to the high expense and complexities of deploying VANET data dissemination techniques in big experiments, an implementation is required with simulators. Three significant challenges can be avoided through VANET simulation. To begin, simulation systems' credibility and feasibility need standardized and accurate simulation parameters that can be verified using different verification methodologies. Second, the models of vehicles mobility must include various levels of complexity to replicate real-time traffic circumstances and driving behaviors. Simulation scalability is a significant issue in this context. To be more precise, it is currently essential to model the entire stack of extremely large VANETs.
5) Efficient buffer management: The salable VANET network can produce a massive number of messages to be disseminated. Vehicles can be used as intermediate relays to forward multiple messages simultaneously in multi-hop dissemination protocols. Most data dissemination solutions assume the optimistic hypothesis that vehicles have an endless buffer and thus do not require a replacement policy. Additionally, they disregard scheduling messages transmission and dropping. While cooperative caching is feasible in wireless networks, it is challenging in VANETs due to the numerous disconnectivity and the challenge of maintaining consistency among several message duplicates. Even though some cooperative caching attempts are present in the VANET [188], it may be interesting to analyze the influence of social relationships among nodes on caching. Additionally, forecasting buffer space is critical, as buffer space is restricted in nodes in the network [189], [190].

### C. VANET RESOURCES MANAGEMENT CHALLENGES

In VANET infrastructure there are many resources that are shared among vehicles such as bandwidth channels and RSUs. This sharing brings many challenges for VANET deployment. This section will introduce the main challenges that are related to VANET resources management.

### D. CHALLENGES OF RADIO RESOURCES ALLOCATION

Medium Access Control (MAC) techniques are critical in ensuring fair channel access for all vehicles while minimizing data packet loss. The main characteristics of VANET, such as highly dynamicity, intermittent connectivity, various QoS requirements, and security challenges, have created several open issues and the need for future works to increase the efficiency of the MAC in the VANET. Despite efforts to improve MAC protocol performance in VANETs, several MAC research concerns and unanswered questions remain to enable VANETs to handle safety and non-safety services. This part identifies several challenges that may be future research topics.

1) Scalability: In different VANET scenarios, vehicles travel at different velocities and so they may join or leave the coverage area of RSUs at any time. The number of vehicles may vary according to many factors such as working time, roads congestions, nearby shopping centers, offices, and others. When the number of vehicles increases, the broadcasted messages will be increased dramatically. However, the MAC protocol should deal with the scalability challenge and provide sufficient bandwidth channels for data transmission even when the number of vehicles increases [191]. A complicated issue to address while creating MAC protocols for VANETs is vehicle mobility, which results in large fluctuations in vehicle densities over time. Furthermore, the changing traffic density induced by increased vehicles mobility significantly affects how the MAC protocols' reliability. When vehicles density is high, a random access time that is too small will affect the quality of MAC protocol. But on the other side, an excessively long duration of the interval will result in unfairness in the access to the bandwidth channels. Thus, to ensure the reliability of a MAC protocol, the period of the random access interval must be continuously modified in accordance with vehicular density and the availability of time slots that can be reserved for vehicles. Therefore, for more efficiency, MAC protocols must consider the number of vehicles. This can be achieved through the development situation aware MAC mechanisms that have the ability to dynamically adapt to multiple changes in traffic density. taking the situational information such as vehicles mobility, working times, and communication requests into account can provide a scalable MAC protocol. Also, predicting vehicle density can enhance the frame in a proactive manner. so, future MAC protocols must be adaptable with more than vehicles density but they also take into account application type and QoS requirements as another improvements factors.
2) Central Coordination Requirements: MAC schemes are constructed in such a way that the channel coordinator, such as RSU or cluster head, must transmit the first packet at the start of the frame. Without a channel coordinator in a limited VANET environment, MAC mechanisms cannot ensure vehicle control and management. So because VANETs never have fixed infrastructures, they lack a centralized coordinator, and control is evenly distributed among the vehicles. Neighboring vehicles will exchange control messages to avoid colliding throughout channel access. Besides, MAC protocols should ensure that the overhead caused by control message broadcasting does not use valuable bandwidth, resulting in poor QoS and more latency.
3) Consideration of many performance metrics: Regretfully, most existing MAC algorithms were developed to optimize the transmission latency for safety services at the cost of other MAC performance metrics [192]. For

complicated applications like multimedia applications, channel access fairness, packet loss rate, and stability are vital performance criteria. Upcoming MAC protocols must improve the trade-off between MAC performance metrics, which is complicated.

4) Application diversity: VANET is meant to provide passengers with many safety and entertaining services. Unfortunately, most MAC protocols surveyed were designed for critical safety services requiring timely message broadcasting between surrounding vehicles [192]. They are focused on a narrow set of applications and cannot support the wide variety of typical applications. This would necessitate the development of a MAC protocol capable of delivering a constrained access latency for safety applications while still delivering wireless data transfer at a suitable data rate for non-safety applications. There are some research findings in this sector; however, they are not entirely satisfactory.
5) Multichannel operation: the heterogeneous VANET communication may utilize different bandwidth channels for data transmission. It can integrate many communication paradigms such as DSRC, LTE, and mmWave communications. On the other hand, most MAC protocols proposed to utilize the seven DSRC channels for vehicular data transfer [32]. It is vital to building MAC protocols that exploit all available channels without interfering with adjacent channels that enable them to be highly scalable.
6) Access Unfairness: Numerous MAC schemes fail to ensure balanced channel access for vehicles passing at different velocities. Vehicles traveling at high speeds have a finite time to get the desired service within a given communication range. This fairness issue may arise regularly in VANETs scenarios with a substantial relative variance in the velocities of various vehicles. On the other side, this problem may be more worst when the MAC protocol is based on applications or services priorities for channels allocation. As a result, this issue must be studied and efficiently solved while creating MAC protocols for VANETs.
7) Mobility scenario: Most MACs were developed for specific scenarios (urban or highway) and do not consider the traffic situations found in urban areas with intersections, buildings, tunnels, and traffic lights, for example. The next generation of MAC protocols should operate in both environments efficiently.
8) Interference between RSUs Several MAC protocols presuppose the existence of RSUs to coordinate channel access among vehicles within their coverage region [193]. Conversely, the works are interested in mitigating the effect of the overlapping area between RSUs that operate in the same frequency band. So, upcoming MAC protocols should include effective inter-RSU communication schemes capable of mitigating the effect of channels interference in the overlapping areas. It should be conducted so that QoS consistency is maintained, particularly when a vehicle leaves/joins an RSU coverage region.
9) Stability of clusters and inter-cluster interference: A significant focus has been dedicated recently to MAC strategies. One vehicle from each group is chosen to design and maintain a timetable for slot assignments. Despite research attempts to boost the effectiveness of cluster-based MACs, numerous difficulties remain unresolved due to the fast dynamic network topology that needs more investigation [193]. Cluster instability can cause MAC to function poorly. Inter-cluster interference, a collisions source, can be managed without reverting to costly spectrum and sophisticated multichannel technologies such as FDMA or CDMA. By developing low-overhead techniques for cluster creation and maintenance, the performance of cluster-based MAC algorithms will be improved.
10) Communication overhead: In large-scale VANETs, vehicles must share information with other surrounding vehicles' about timeslot availability, code use, and SCH number. This will raise communication overhead and degrade transmission performance [192]. Without RSU control, vehicles use the channel freely. There is no fixed assignment, which raises the risk of packet collisions to a certain level, particularly during periods of dense traffic. The centralized MAC schemes handle the CHs or RSUs scheduling, which is advantageous for configuring non-intersecting access channels. Centralized MAC protocols offer a lower communication overhead than distributed MAC protocols.
11) Location Awareness: Many applications in VANET networks are location-dependent [30]. Even location estimation, sharing, and awareness among vehicles are required for data collision-free operations. MAC protocols designed for the VANET network should not rely only on GPS signals but should use prediction and estimation facilities for transmissions. Relying on a single infrastructure for location input can fail the whole mission. For example, the GPS signal can be hacked and doesn't operate properly in all scenarios, such as tunnels, high buildings, bad weather, etc.

#### 1) VANET INFRASTRUCTURE DEPLOYMENT CHALLENGES

Effective resource management solutions such as storage optimization, bandwidth control, and messages scheduling are essential to assuring equality in resource deployments to maintain diverse applications in various vehicular situations.

1) Load balancing. As a result of the rapid advancement of vehicular telematics, modern vehicles are generally interconnected via heterogeneous radio access models and can exchange vast amounts of data with their environment. That data requires more processing in terms of security, compression, and further analysis, resulting in higher loads on the RSUs [194]. To handle such a scalable computation load, there are a number of

methods and solutions were suggested in the literature. Load balancing can ensure more fairness, reliability, and the least percentage of system breakdown. The improvements in the internal hardware of RSUs and the development of efficient hardware management policies may solve some of the problems [194]. Also, the deployment of many RSUs to deal with scalable computation load can minimize the traffic load but it will bring more challenges of management, handover, and costly [195]. However, the load balancing in VANETs is more serious due to the requirements of time-critical applications. Different VANET data processing such as routing selection, security verification, and decisions making should be achieved in a timely manner. The primary goal of load balancing is to allocate resources in order to maximize performance and decrease latency. The applications such as traffic congestion messages, accidents alarms dissemination, and traffic improvement should be delivered with minimum delay through achieving the fault tolerance load distribution. Balancing the load between all the vehicles is one of the problems in VANET that requires more attention.

2) VANET infrastructure Security: VANET infrastructure security represents one of the main concerns that face the deployment of VANET around the world. Due to its relationship with human safety and transportation management, VANET should be secured against hardware and software vulnerabilities [1], [67] due to its association with human safety and transportation management. RSUs are the main component of VANET infrastructure which are responsible for vehicular data management, safety message dissemination, traffic data analysis, and provision of the transportation authorities with vehicular data. The RSUs should be protected against any exploitable weakness in their system that enables attack through remote or physical access to VANET data. RSUs should be secured against any attacks exploiting interaction with an RSU's electronic components [95]. Also, it should be secured against the access of unauthorized nodes and malicious modules. Hackers may use V2I communications to provide RSUs with invalid messages or malicious instructions to attack the databases or management software. However, RSUs security requires more research effort to answer many research questions related to the degree of security requirements against both the hardware and software threats. Also, the rapid movement of vehicles and high mobility make them move quickly from an area of different RSUs. In any case, vehicles moving from an RSU to another RSU will bring with them several security problems, for example, vehicles authentication, vehicles privacy, and secret keys management. However, the exchange of these data among RSUs may bring many security threats and challenges associated with frequent handovers causing an increase in the packets delivery rate.

3) Data offloading: Often in crowded cities and workplaces, vehicles can increase unexpectedly, causing significant overloading on the resident RSUs. This overloading may lead to a high delay in data transmission, thus reducing the QoS. Many of the suggested solutions that can be used here exploit the computation abilities of parked or slow-moving vehicles to offload the calculations to them. It is also possible to take advantage of the high computing capabilities of nearby infrastructures such as cellular networks. Data offloading can be helpful in VANET for reducing network overload, as it not only produces reasonable data management solutions for congestion mitigation but also provides the VANET with a large capacity for introducing more services. Offloading VANET data is a relatively new and active research field. Even with all these studies that have been conducted [196], there are still numerous outstanding research issues associated with the use of data offloading technologies. One of the primary obstacles to VANET data offloading is a scarcity of global information about the network. To improve the effectiveness of the first seed selection process, it is critical for RSUs and vehicles to acquire global network information, such as social interactions, congestion conditions, buffer levels, and traffic patterns. However, some vehicles and neighboring infrastructures are unwilling to share their local or private information with others for security and privacy reasons [197]. While several existing industry standards have attempted to give further network information, sharing complete information remains a work in progress. Another issue that arises when offloading VANET data is the absence of realistic node demands and behaviors. The service provider must build appropriate incentive schemes to induce nodes to participate in the data offloading process. Furthermore, it is difficult for the service provider to precisely predict the nodes' requests and behavior, which considerably impacts the data offloading performance.

4) RSUs localization. In VANET communication, the RSUs should be deployed around the roadside to collect the required data, analyze it, and provide Internet and cloud access to nearby vehicles. The RSUs should be deployed in optimal locations with minimum signal blockage, high electromagnetic interference with nearby BSs or RSUs, and high transmission gain with the covered area. Unfortunately, the random distribution of RSUs may lead to many network disconnections and scalability issues. However, RSUs localization schemes are required more improvements to determine the necessary number of RSUs that each area needs and how they are distributed and located around that area. For real-time applications, the RSUs localization models should take into account a number of factors such as vehicular density, congestion times,

and covered area information such as buildings and other infrastructures locations. The RSUs number certainly increases on crowded roads and intersections, decreasing on highway roads. Due to its cost-effective and 3D mobility, some works are suggested to use the UAVs as flying RSUs in the high congestion or less-infrastructure areas to handle the increased communication requests and mitigate the blockage and infrastructure issues [15], [198]. It is noteworthy that those works are in the beginning and have not been practically tested. Also, UAVs have many inherited issues such as power limitation, collision avoidance, and control problems that make their deployment in VANET a significant challenge [18].

5) Heterogeneous Communication: in future VANET, a number of different modules and infrastructures can be integrated to provide V2X communication, such as BSs, UAVs, and pedestrians' handhelds. This heterogeneity will improve human safety and public transportation systems by providing different methods for collecting additional vehicle mobility data, disseminating safety messages, predicting vehicular density, and making optimal decisions [33]. More challenges come with this communication that needs to be solved, such as data security, data compatibility, infrastructure usage costs, complexity management, data usability, and transmission synchronization.

6) Caching optimization: The RSU serves as a router, server, buffer, and data backup and recovery system, providing various services to the clients and storing information about the currently connected vehicle in the network. Practically, each vehicle should provide context information such as velocity, direction, and GPS location to nearly RSU through periodic beacons. RSUs will store these data to be used for further analysis for vehicular density estimation, data dissemination, and data forwarding. Also, RSUs can be used in many tasks related to managing the public transportation system. For example, it can disseminate critical messages to nearby vehicles to avoid traffic jams or potential accidents through V2I communication. RSU can also be used as an intermediary for exchanging data between vehicles through multi-hop communications or to provide an Internet connection for vehicles within its transmission range. However, these services can produce vast amounts of data overloading the RSU storage system. Correspondingly, this data may be useless after a definite time due to the nature of the transportation system that frequently changes [199]. Optimal cache replacement and compression methods can be helpful to overcome such challenges [200]. As a result, there is crucial to develop intelligent models to optimize data storage in RSUs and deal with data validity and redundancy.

7) Requests Scheduling: In the VANET, the RSUs may receive many requests such as Internet access, data dissemination, multi-hop data transmission, and other services access. However, the access of multiple requests simultaneously will cause a high burden on the RSU and increase the execution time. As a result, there is an urgent need to develop scheduling algorithms that can deal with the massive number of requests in an efficient and timely manner. Therefore, scheduling data is crucial to serve as many requests as possible, reduce the delay of data delivery, and improve network throughput. Scheduling is an essential issue for data access in a vehicular environment. Numerous factors influence the scheduling of VANET data, including the request valid time, the request inter-arrival time, the data access structure, vehicle velocity, the workload impact, and the hotspot effect [146]. Moreover, the scheduling algorithms can utilize the service type and vehicle context information to create a priority-aware scheduling algorithm. Emergency applications receive a greater priority than non-emergency applications. This results in user advantages and increased throughput. Developing data scheduling algorithms that can serve both the safety and non-safety data requests on time is a big challenge.

8) Costs of VANET Infrastructure Improvement: to optimize VANET communication in terms of delay reduction and data rates increasing, there are many works related to optimizing vehicular communication through integrating new emerging technologies such as 5G, SDN, UAVs, Fog computing, MEC, and others with VANET communication [59], [87]. However, all of these solutions require more costs for their deployment, management, and security [19], [74], [87]. The compatibility and applicability of emerging technologies may require some modifications and additional software. However, to our best knowledge, there are no suggestions or surveys to study and develop economic models to investigate the costs of integrating emerging technologies with VANET networks in terms of time, money, and effort.

9) Real-Time Implementation: Many VANET protocols and solutions are suggested and verified through simulation and testbeds tools. Though the simulation methods can provide good results in determining the deficiencies and weaknesses in the model before deploying it, many issues and challenges may appear in the real-time implementation. For instance, many of the data routing protocols are verified with high results in terms of packet delivery latency and throughput in the simulation status, but they didn't take into account the signal interference, vehicles willingness, and weather effects on the data transmission. Also, some of the challenges related to governmental laws and security

permissions may obstruct the deployment of VANET infrastructure systems.

### 2) C-V2X COMMUNICATION CHALLENGES

To ensure that vehicles can access the VANET services, even in areas where RSUs have not been deployed, various wireless access infrastructures such as mobile networks (3G/LTE and 5G) and Wi-Fi could be used to provide VANET services. This will conduct what is known as a heterogeneous vehicular network based on utilizing a combination of DSRC and other wireless networks to offer vehicular communication. DSRC is incompatible with V2X applications that require data transmission to be with minimum latency for high coverage areas. The second significant limitation in DSRC is the small number of channels involved, which results in increased network congestion and latency.

Conversely, cellular technologies do not have this limitation, as the BSs have a more excellent network coverage than the DSRC technology. The cellular V2X communications provide several benefits, including increasing the network's capacity, lowering the cost of deploying additional infrastructures, increasing the VANET's overall reliability, and increasing the system's flexibility by providing services for both short-range and long-range services. Additionally, cellular communications can give a wide coverage area, which reduces horizontal handover, as the communication between the vehicle and the base station is longer than the connection between the vehicle and the RSU. At the moment, there are many challenges behind such hybrid communication, including the following:

1) Handover control: Due to the mobility of vehicles, multiple handovers will result. These fast handovers cause more challenges in conventional systems' resource allocation, resulting in significant overhead and latency. When vehicles travel within the transmission range of RSUs or BSs, there is a rapid alteration in the points of attachment (PoA) of the RSUs or BSs [201]. Essentially, when a vehicle goes from an RSU-covered area to a BS-covered site or vice versa, data is transferred in varied PoAs utilizing various access protocols. Vertical handover is used to describe this type of handover [202]. Vertical handover is particularly complex since different access technologies differ in terms of the radio spectrum, bandwidth, modulation techniques, and so on. Additionally, the vehicles cannot communicate during this phase until registration is completed and data security and authentication verifications are performed. As a result, a robust handover mechanism that ensures seamless connectivity is critical. Machine learning-assisted techniques can assist in predicting vehicle movement and allocating resources appropriately. Those that don't demand prior knowledge of the vehicular environment, like reinforcement learning (RL), should be prioritized [203]. Also, as claimed in [204], cell-free communications, which lack cell borders, can enable uninterrupted vehicle mobility. All of these methods are still in their infancy and lack real-time implementations.
2) Efficient network discovery/selection: During its journey, vehicles may travel through several heterogeneous small networks, and due to their high speeds, the likelihood of falling outside the coverage area of the underlying network is considerable. The discovery of an efficient network is essential to reduce the time required to discover network routes and enable rapid handover. However, before deciding, the network selection mechanisms should consider user-centric or network-centric requirements. The user-centric decisions rely on economic implications (i.e., whether to use the cellular network, which is accessible to subscribers with varying data plans, or the DSRC technology, which is relatively free) and QoS metrics like delay, packet drop, application-specific requirement, and so on) [29]. Conversely, network-centric causes include the following: data-traffic prioritization, load balancing based on RSU/BS capacity, fairness, and power optimization. An effective network selection strategy is needed to minimize network association time and connectivity problems. Due to limited or erroneous local information on the vehicles, the network selection strategy may make poor handover decisions [201]. However, using machine learning models to assist in network selection derived from past and situational information can lead to high QoS metrics, for which further study is being conducted.
3) Security: In V2X communications, the cellular infrastructure may be used for data delivery among vehicles and RSUs or among vehicles themselves. Also, it may be useful for vehicles to access the services of cellular networks such as Internet access, locational advertisements, and IPTV [201]. However, the security vulnerability of both networks will be a big challenge. Without considering the security constraint, the cellular infrastructure can reach or change the data stored on other vehicles. Hereafter, the sensitive information stored on vehicles must be secure to keep it against unauthorized access. The utilization of cellular infrastructure without any security reliability may expose the VANET infrastructure to more risks. For most vehicular services, vehicles may broadcast their sensitive data such as GPS location, ID, mobility pattern, etc. which should be private and secured. Access to such data by the cellular network may be risky and lead to high-security threats. There are two basic categories of potential security issues: attack on the user and attack on the network. Attacks on the user cause traffic congestion, car crashes, and push drivers to make poor judgments, whilst attacks on the network record the vehicles' local information and create erroneous reports of misconduct, reducing the system's reliability and efficiency [29]. Also, the cellular network will be at risk situation if its data and services

are accessed from abroad, for example by vehicles. Suspicious vehicles may send data containing hacking codes or disrupt the network resources, which leads to the disruption of some of its services and harm to its users. As it is known, each network infrastructure can operate with a security system that differs from the other in different network infrastructures, so it is necessary to find an integrated system that works to settle the difference between the two infrastructures. Also, there are many security challenges that appear with this integration, for example, keys management, privacy protection, and authentication verifications. The existing VANET security solution has the use of temporary pseudonyms for vehicles identification. Additionally, location-based encryption is employed to maintain location privacy [23]. In contrast, cellular networks issue each subscriber a separate hardware-based identity Subscriber Identification Module (SIM) for identity verification. Furthermore, privacy constraints and verification approaches should be researched further in C-V2X communications. To address security concerns, scientists should develop innovative highly secured protocols that can be explored through the perspective of heterogeneous vehicular networks' characteristics.
4) Coexistence and collaboration amongst diverse networks: Future generations of ITSs are expected to take a more widespread approach to network solutions. This will necessitate support for the coexistence of many nearby wireless infrastructures to supply global access to different services. Cooperation between cellular networks, for example, will enable travelers to access valuable services such as information on traffic situations, routes, and climate changes. Cognitive radio technology can enable cooperative communication between VANETs and cellular systems [10], [46]. Recent research indicates that cognitive radio enables more cooperative communications without impairing cellular services [11], [205]. The invention of radio resource management, link adaptation, and relay selection is critical for system performance improvement in cooperative communications. Additionally, resource management must be considered in heterogeneous C-V2X networks to improve resource usage, reliability, and resilience.
5) Infrastructure and Economic Considerations: Although the mobile network infrastructure has been operational, providing extensive network coverage, high data rates, and capacity, there are also economic impediments to providing uninterrupted V2X service via cellular communication. In a VANET, vehicles generate a considerable amount of data due to their interactions with other vehicles and their environment. Utilizing a cellular infrastructure for this type of communication will never be free, and users may be required to pay for data plans. The cost of hardware is critical, and hence service providers must provide a practical economic model that is appealing to users. It is vital because it will directly impact the expansion of such integration and consumer interest. Both systems have tremendous promise for implementing V2X communications in the real world, but each also introduces a slew of challenges that must be addressed before deployment becomes feasible. One such limitation is the requirement for continuous nationwide network connectivity. Utilizing cellular architecture for VANET data management and delivery places a significant load on the cellular system and may significantly decrease the QoS delivered. As a result, it is vital to develop strategies and models that enable cellular systems and compensate for the service supplied to the VANET by its infrastructures. Consumers' options may be formed from existing business models such as pay-as-you-go, pay-per-use, and pay-per-service. In contrast, storage and processing are also critical considerations for service providers. Designing a rewarding economic model that can assist the incorporation of cellular and DSRC technology requires more research attention.
6) Simulation platform: both networking models, cellular and DSRC, have different properties in terms of signal coding, MAC, congestion handling, and more. Thus, determining a general simulation platform that contains typical vehicular network scenarios and V2X use cases is in great need to provide fair evaluations and comparisons. Moreover, security analysis and scalability study could be done systematically with such a generalized simulation platform.

## VII. VOLUTIONARY TECHNOLOGIES and FUTURE RESEARCH DIRECTIONS

This section will discuss various technologies that can be characterized as evolutionary. While they have matured over time due to substantial research, testing, and deployment, significant additional development and trials are required to adapt them to the new problems and requirements of upcoming VANET services.

### A. REAL-TIME BIG VEHICULAR DATA MANAGEMENT

With thousands of vehicles on the road, various network participants generate a massive amount of data. These vehicles are equipped with several sensors, which create an enormous amount of data instantaneously. Additionally, the proliferation of sensing systems in the transportation environment, such as sensors installed on roadways, roadside surveillance cameras, and others, has resulted in the generation of vast amounts of data. These big amounts of data should have been managed and integrated to maintain bandwidth and capacity. Likewise, real-time data retrieval from big data has become a challenge. This problem is related to many challenges, including computing overhead, time consumption related to big data analysis, and data interoperability from several sensors.

Generally, big data is decentralized physically and logically but theoretically centralized [33]. The management of this vast amount of dynamic data entails many activities, including data collection, processing, storage, validation, accessibility, and distribution. The volume of data produced by VANET applications, on the other hand, is far too large to be processed by traditional algorithms and approaches. Also, transportation data may be erroneous, outdated, or unreliable in specific areas or times due to the continuous mobility of vehicles and passengers. For example, not every vehicle is equipped with the technologies necessary to get real-time position data, and traffic data collected by road sensors may be lacking.

Also, At the moment, data volume has grown from TB to PB, and data storage capacity development is lagging far behind. Conventional data storage systems and database technologies are incapable of dealing with the growing volume and complexity of massive VANET data [203].

As a result, developing the most rational data storage systems has become a critical task. Additionally, timeliness is essential for big data usage in VANETs, including preprocessing, traffic state classification, real-time bus scheduling, traffic control, and dynamic route guiding. Traffic data in various forms from various sources should be similar to past data and then processed quickly [206]. The data processing units should be capable of processing increasingly complex and growing data. Ensuring process timeliness while dealing with such vast and fast data sets is a significant concern.

Other issues confronted extensive data processing due to sensor data redundancy, anomalies, and granularity. For this purpose, the VANET requires an effective and real-time data management system. To enable VANET service users and application developers to efficiently access and reuse data, data must be stored and made publically accessible with a high degree of correctness, accuracy, reliability, and consistency [207]. Big Data will be deceptive without high-quality data and may even yield adverse effects. Really, for aggregate, process, and analyze data in heterogeneous vehicular networks [32].

To this purpose and in order to address these issues, numerous solutions, such as cloud and fog computing, have been proposed but are still in their infancy [206], [207], [208]. Vehicular clouds/fog computing enables efficient utilization of vehicles' computation and storage resources. Thus, substantial attention must be made in the future to providing real-time big vehicular data administration via the application of various ML algorithms and data analysis strategies that enable the provision of effective delay-aware big data management alternatives. Additionally, crowd-sourcing and crowd-sensing may play a critical role in the future management of VANET big data [209], [210].

### B. IOT-DRIVEN VANET IMPROVEMENT

The number of moving vehicles has already been quickly increasing in recent years, resulting in traffic congestion and rising ITS shortcomings. VANETs have advanced significantly as wireless technology and the Internet of Things (IoT) has advanced. VANET has been widely used with the help of IoT for both safety-related and non-safety-related applications to assure traffic safety and reliability [211], [212]. It is based on the concept of creating smart cities in which VANET systems are linked to IoT to keep data on the internet, also known as the cloud. So, IoT-driven VANET will create a new era in vehicular communication.

Future IoT-based ITS will provide necessary real-time actions to vehicles or drivers [213]. Introducing IoT into the VANET should increase flexibility, latency minimization, and high bandwidth connectivity. VANETs and IoT can provide a wide range of services and solutions that add value to people's lives by delivering comfort, enhanced accessibility, and improved citizenship, as well as asset protection and safety [214].

However, different sensors and vision systems must be deployed and connected to RSUs in VANET-IoT systems to collect and aggregate sensory information about the local environment. This information is then delivered to RSUs for analysis to ensure effective and consistent traffic flow. Apart from monitoring, the RSUs can also send emergency notifications to neighboring vehicles and agencies. While this aggregated data is beneficial in the limited context, for instance, in improving traffic accident detection and avoidance, as well as data forwarding and dissemination, it is often forwarded to the cloud platform for long-term storage and analysis to bring insights and predict related to requirements of smart city transportations.

Also, fog computing can be used to construct an effective framework for processing data and making decisions to accomplish the surveillance purpose with the least latency.

According to certain studies, like in [215], they combined IoT, WSN, and VANET to prevent vehicle collisions, provide warning notifications, and avoid traffic in work zones. Additionally, the authors of [216] suggested utilizing IoT and VANET frameworks to ensure the safety of mining workers by enabling machines and vehicles circulating in an underground mine gallery to exchange their locations; their path traveled, incident detection messages, and automated emergency braking mechanisms, and update traffic data.

The Internet of Things will monitor workers' health hazards, physical activity, exposure to fire, extreme heat and humidity, and dust and gas-phase dangerous compounds. In the next few days, the VANETs need to enable the development of a broader range of real-time traffic safety applications, potentially saving countless human lives. Significant efforts have been made to enable VANET-IoT applications in various scenarios. These include drivers e-health monitoring, monitoring and checking driver behavior, route planning, weather forecasting and analysis, intelligent traffic lights, undisciplined driving diagnostics, accessible parking areas, and other location-aware information such as road status and traffic.

In this regard, VANET should use IoT to provide personalized safety features such as the detection of personal health conditions and anti-fatigue frameworks while driving, the recognition and classification of driver emotions while driving (stress, inebriation, etc.), and the awareness of possibly dangerous objects that cross a road such as walkers, animals, and so on [217], [218]. Eventually, the cognitive IoT must be connected with the VANET to enable such applications through utilizing cognitive computing systems on the data generated by sensors and devices.

By using multifunctional sensors and ML techniques to analyze the surrounding environment and monitor driver actions and health status proactively, the integration of VANET and C-IoT can yield significant benefits in terms of road safety and improvement. Nevertheless, this integration will require additional effort to address the issues of multi-sensor data collecting, data analysis, sensors and devices localization, data processing and transmission on a timely basis, and how the VANET-CIOT paradigm will make context-aware decisions. Both C-IoT and VANET produce a diverse set of data with a range of distinct purposes and changing frequency in terms of speed and volume.

As a result, data collecting across multiple platforms requires more intelligent pre-processing of the data on the local level. Additionally, VANETs communicate using DSRC, whereas IoT utilizes a diverse set of communication protocols, including NFC, Bluetooth, and WiFi, as well as protocols based on well-known standards like MQTT, Z-wave, RPL, CoAP, Neul, Zigbee, Sigfox, 6LowPAN, and LoRaWAN [219]. The protocol compatibility, handshake negotiations, data rates, and other such aspects all contribute to the total performance of dependent services. In this context, the diverse characteristics of these different systems imply trade-offs and research of each.

Recently, Cellular IoT has been presented to utilize unused spectrum in cellular communications and transmit across them. This cellular Internet of Things technology was described as a replacement for unlicensed LPWAN, LoRaWAN, and Sigfox [219]. Not only can integrating cellular IoT into VANETs cut power consumption, but it also simplifies implementation complexity and costs. Cancellation of RSUs requires a specialized infrastructure developed exclusively for VANETs, with cellular towers serving as RSUs. Additionally, as new cellular technologies become available, new technology can modernize cellular IoT [220]. Another significant problem for this integration is data security and privacy.

Because devices in IoT-based VANETs are connected via various hardware and software, data privacy, security, timeliness authentications, and location privacy are all at risk of illegal manipulation and exploitation, particularly at crossings in congested urban areas. It's worth noting that data created by IoT networks are inherently private, necessitating the use of privacy-preserving methods. Without that robust privacy protections, sharing IoT data readily results in end-user privacy violations. Additionally, context-aware privacy-preserving mechanisms must be implemented to enable VANETs clouds to accommodate the shift.

Lately, Narrowband-IoT (NB-IoT) technology is broadly recognized as a division of the traditional IoT technology. As compared with other low-power wide-area IoT technologies, NB-IoT has larger coverage area and ultra-low energy requirements [221]. Cellular networks represent the basis of NB-IoT network system, reducing the costs of network deployment. NB-IoT is deployed on the basis of a Low Power Wide Area Network (LPWAN) standard that is innovated mainly to interconnect a wide range of IoT devices and services. NB-IoT uses only one narrow-band of 180 kHz [221]. From the beneficial analysis, it can be concluded that the benefits of NB-IoT in ITS applications are very recognizable. Urban traffic congestion can be alleviated by the development of various intelligent transportation solutions. As a result of the implementation of NB-IoT, transportation has become more intelligent. Third-party application software allows users to get real-time vehicle location data, do information searches, and reserve parking spaces [222]. The emergence of NB-IoT technology may strengthen a variety of connections between the vehicle and the outside world. This new technology has only been established in the last few years, therefore the research and development system for it as well as its use in smart transportation are still in development stages, and certain problems will inevitability appear in real-time deployment [222]. A number of issues that should be addressed in future research such as a high number of NB-IoT devices requires dynamic network access, therefore the development of multiplayer scenario can enhance the system throughput. Also, the high dynamic of IoV topology could increase the challenges of cooperative relay system for NB-IoT physical uplink shared channel. Besides, the fully utilization of NB-IoT in IoV environment requires more consideration that need to be considered such as communication models, packet scheduling, power control, network delay and number of repetitions.

### C. HETEROGENEOUS IOV

The introduction of ITSs and the pressing need to increase connectivity, availability, and integrity with other infrastructures have facilitated various studies on vehicular communications development. The internet of vehicles (IoV) is another revolution in vehicular communications that is rapidly gaining traction in transportation. IoV is concerned with integrating the human–vehicle–object–the environment into one platform. IoV helps vehicles communicate intelligently with self-configuring functionalities based on a variety of communication standards and protocols, including sensing, Bluetooth, DSRC, Mobile broadband, RFID, Wi-Fi, and GPS.

IoV is critical for ITS development by increasing the capacity and scalability of existing VANET networks. Nowadays, IEEE 802.11p and wireless communications via V2V and V2I communications are used mainly in the existing VANET [129]. Emerging IoV applications necessitate different wireless interfaces to minimize transmission costs. Although DSRC is cost-effective, the coverage area may incur a greater cost due to the use of various network interfaces such as 802.11ac, Wi-Fi, LTE, mmWave, and 4G/5G

[223]. The nodes contributing to IoV communications are generally heterogeneous, such as vehicles, couches, traffic signals, lorries, bicycles, RSUs, portable devices, and other local computing infrastructure. The diversity of these nodes results from their different data communication, dependability, computing, accessibility, cybersecurity, and storage requirements [33].

Apart from the big data requirements of upcoming IoV applications and the pressing need to accomplish data analysis and delivery with minimal latency and large throughput, researchers seek to optimize the analysis, forwarding, encoding, protecting, availability, and storage of IoV data by leveraging the high capabilities of emerging technologies such as fog computing, MEC, SDN, and blockchain [224], [225], [226], [227], [228]. Also, the manageability of many nodes/devices in a heterogeneous IoV infrastructure without decreasing data transmission performance or growing data processing complexity is viewed as difficult in this domain. Notably, such diversity in nodes and techniques, in addition to the many modalities of communication, necessitates the development of different processes and standards models to assure the network's reliability and proper operation.

Also, the heterogeneity of IoV infrastructure will subject the critical safety-related data to various security threats and cyberattacks. Furthermore, the massive volume of data generated in the heterogeneous IoV is transmitted and stored by various entities, including vehicles, RSUs, BSs, fog systems, cloud datacenters, and SDN controllers distributed across numerous decentralized nodes. This will make the data more vulnerable to attacks and authentication challenges. As a result, security and privacy concerns necessitate the development of scalable security mechanisms and architectures that enhance effective network connectivity and storage in such platforms while maintaining authentication, secrecy, privacy, and integrity. Standardization and device compatibility are also significant tasks in this area.

Various challenges are required to be standardized, such as processing capabilities, storage, power usage, frequency spectrum, and protocols and communication stacks [224]. Lack of communication standardization and device interoperability imposes significant constraints on IoV communication development, which the vehicular communication sector might address. Resource allocation is a critical component of a heterogeneous IoV framework that supports both effectiveness and cost of network maintenance. Appropriate resource allocation enhances the performance of both the IoV network and the quality of offered services. It helps avoid the many temporary bottlenecks that occur in the IoV. However, these primarily include bandwidth, processing units, RSUs, BSs, cloud servers, and SDN controllers.

Recently, content-aware resource allocation solutions that consider the workload and popular distribution of units while determining the required resources can be utilized to assign resources following service requirements. Users have varying content requirements for various apps running across IoVs. Utilizing such requirements will provide better results. For more optimality, the content-aware resource allocation method should take into account a variety of constraints and requirements such as the available resources and their associated costs and networking statistics such as content validity, kinematic vehicle information, connectivity stability, and link status information. In recent times, machine learning techniques, particularly DL and RL, have provided novel solutions to low-complexity resource allocation problems [229], [230], [231].

In VANETs, various critical characteristics of applications and customers, such as customer requirement, network parameters, and resource use, may be predicted and modeled using intelligent methods. Additionally, the extracted features can be used to optimize resource allocation. As a result, how to properly model and predict the resource allocation problem to optimize the performance and scalability remains an unanswered one. Apart from that, depending on the structure of the heterogeneous IoV network, a significant number of vehicles and network nodes may be deployed to ensure effective VANET connectivity and localization. in such a scenario, routing strategies should be scalable and intelligently built to deliver the messages in this environment. It should optimize the decimation of data. Additionally, the routing protocol should be capable of locating and recovering lost data packets in a vast network. These assumptions necessitate the use of a more sophisticated routing system.

Additionally, the greater the number of vehicles interacting at any given time, the greater the bandwidth required. As a result, an appropriate technique is necessary for reducing usage bandwidth through intelligent memory allocation techniques. This requires effective data accumulation, allocation, and validation management. As a result, this issue remains unresolved in heterogeneous IoV. Dealing with these issues in a wide-scale IoV network is an open subject that academics should investigate due to the enormous number of vehicles, networking technologies, and smart objects distributed across large regions.

### D. NETWORK GLOBALIZATION

Nowadays, the world has become a small village, so it is possible to move and travel by personal vehicle to any possible destination inside or outside the country. In the VANET communication, a unique pseudonym number should be assigned temporarily to allow each vehicle to participate in VANET applications and services. These pseudonym numbers are given as long as the vehicle moves within the VANET covered area that will be updated frequently for security purposes and privacy preservation [34]. For the best results, the deployment of complete information of the vehicles such as type, model, size, and manufacturer with fixed identifiers numbers within the VANET network instead of temporary pseudonym numbers will benefit in the building of global knowledge about vehicles behaviors (e.g., velocity, followed lanes, stopped zones, etc.), frequent routes, regular communication requirements, and daily access applications.

Additionally, vehicles should submit annual inspection reports, tax payment status, and a record of services, among other things. Vehicles will have Internet-based identifiers, significantly complicating the operation of fraudulently registered, trafficked, and illegally customized vehicles and enhancing the general security and credibility [232]. In aggregate, this will result in cost savings associated with transportation and logistics. Also, this can be useful in determining and estimating the future requirements of services and network resources for each vehicle by studying its frequent behavior and daily activities.

Furthermore, the network authorities can benefit from this globalization facility in predicting the daily traffic load and networking requirements and assigning the optimal network resources without affecting the network performance and QoS. Generally, this will incorporate network performance improvements, energy consumption, and cost minimizations. Also, now the security problems around the world and terrorist plots are primarily carried out through vehicles for transportation, attacks, assassinations, booby-traps, and detonation from a distance. However, through the VANET network, such vehicles can be navigated and localized to detect or possibly prevent security concerns. Also, the embedded sensor systems can help monitor the behavior of drivers or travelers when they intend to do some security or laws concerns.

It is essential to share the VANET data among VANET infrastructures inside the same city or outside with the nearby cities, metropolises, or even countries for data management, networking improvements, technical requirements, and security purposes. However, the VANET should provide direct links with hospitals managements, security authorities, schools administrations, and other infrastructures. Unfortunately, the adoption of the globalization idea collides with many obstacles and problems, such as self-privacy, as most people do not like to share complete information about their movements and trips.

Therefore, an appropriate model must be found to compromise self-privacy and the need to track vehicle information. Also, the problem of data management will be more pressing as the information will be distributed in decentralized servers. It is worth noting that the big data produced by the significant number of vehicles and their continuous movement will create massive data that requires high-efficiency paradigms for processing, communication, storage, security, and analysis. Finally, this network globalization will contradict many of the laws and customs of countries and personal freedom, so legislating laws that allow global data in the VANET has become necessary for administrative, technical, and security reasons.

### E. SOFTWARIZATION AND VIRTUALIZATION AWARENESS PARADIGMS

To meet the massive demand for ultra-reliable low-latency communication (URLLC) in V2X networks, networking operators and telecommunications companies have been pressed to update their infrastructure and data, access models. This will improve the creativity and adaptability of such networks' offerings and programmability [233]. Various paradigms have been offered to accomplish this. For instance, softwarization techniques like software-defined networking (SDN) were recommended as a possible solution for network administration, reliability, scalability, and adaptability [234], [235].

The advantage of using SDN for V2X communication is that any entities involved in the connection, such as RSUs, vehicles, and infrastructure, can operate as SDN switches [236], [237]. Additionally, by using an SDN-based architecture, numerous government agencies and automobile manufacturers can provide many services while leveraging the fundamental vehicular network infrastructure in an abstracted manner [237]. SDN can be implemented further as part of a full solution for building an effective and robust V2X network. For instance, global SDN controllers can manage many network slices associated with different applications. However, the global SDN controller can manage inter-slice communications, and local SDN controllers are used for intra-slice networks management. But, deciding between a global SDN design and a hierarchical SDN design presents a significant issue. The degree of signaling overhead produced by the global SDN network would be tremendous, particularly resulting in a significant number of connected vehicles.

Additionally, because the global SDN controller is a single point of failure, predicting and determining the failure conditions and the situations of SDN system overload needs additional study work. Conversely, the hierarchical SDN design facilities the distribution of signaling overhead between the slice controllers and the global controller at the cost of less efficient resource sharing and allocation considerations. SDN and supervised ML techniques can enable the utilization of multiple access techniques by determining which access technique to be used at any given time and how to allow the sharing of the available resources based on QoS/QoE requirements, network conditions, signal strength, congestion rates, and performance parameters, or a combination of these. Moreover, SDN can efficiently allocate channels and determine the ideal data forwarding path. As a result, a productive routing algorithm for VANETs may be presented that uses the vehicle's position and topology prediction via the SDN controller. For more efficiency, the routing protocol should consider the channel capacity and significant features of the VANET environment in the forwarding decisions.

Consequently, software-defined perimeters (SDP) have the potential to play a critical role in securing vehicular communications. SDP can address a number of the security and privacy concerns that future networks will face. This architecture is based on the need-to-know principle, in which the device's identity is validated and authenticated before access to the application infrastructure is provided [238], [239]. SDP can assist in mitigating a variety of network-based threats, including server scanning, denial of service attacks, password hacking, and man-in-the-middle attacks [239]. SDP can be essential in ensuring the security of V2I and V2N connections [235].

In this situation, the availability of an SDP architecture would have mitigated the attacking attempts by enabling the V2N or V2I communication mode at the base station or RSU, respectively. By locating the gateway nearby RSUs or BSs, the attackers' packets would be discarded at the gateway before being passed to the vehicle, denying the attackers accessibility and preventing them from tampering with the vehicle, such as turning it off. One consideration for SDP design is its resilience.

Due to the proposed SDP architecture's centralized structure, it is also susceptible to server failure. As a result, it is important to implement redundancy methods for the SDP controller to ensure its functionality is not affected. Virtualization seems to be another innovation that can significantly improve the effectiveness and efficiency of V2X communications [237]. This contributes to the network's flexibility and scalability while also decreasing development timelines and associated expenses.

Cloud/edge computing and Network Function Virtualization (NFV) could increase vehicular connectivity by enabling better network throughputs and lower latency, hence enabling essential ITS system services to be supported [235]. Still, given the increased possibility of delays related to cloud computing and the high service requirements associated with V2X networking, the edge computing architecture appeared like a reasonable option [22].

Edge computing seeks to provide distributed processing and storage at the network's edge rather than its core [235]. This results in decreased latencies necessary for safety-related and location-aware applications [232]. Thus, combining cloud and edge computing can significantly improve V2X communication by complementing one another and supporting a larger array of services and applications [22]. Edge computing is particularly well-suited for location-based applications such as traffic analysis at intersections and vehicular density estimation [144].

Despite current efforts to analyze and improve the impact of cloud and edge computing on V2X communications, much more can be done. One example is providing a collaborative distributed computing paradigm between the cloud and the edge of the service-aware facility. Specifically, based on the services provided, some computations can be performed in the cloud for delay-tolerant services, while others should be performed at the edge for delay-constrained applications. however, the computations for speed restrictions, congested roads, and traffic situations can be performed at edge nodes like BSs and RSUs, which are more delay-constrained and require instantaneous sharing with vehicles.

Another application is the transmission and caching of distributed content. This is especially relevant for non-safety and entertainment applications. In this scenario, popular images and videos for a specific region can be cached locally at edge nodes to minimize the access latency. Furthermore, these applications introduce numerous issues, such as server positioning decisions that must take into account multiple criteria such as service latency needs, QoS/QoE realization, and computational requirements of the services and applications. Additionally, NFV is another technology with massive potential for V2X communications improvements. This is enormously advantageous since it results in more popular platforms, increased adaptability, and quicker development times [237].

According to V2X connectivity, NFV can support the update and maintenance of new applications for intelligent onboard systems (IOSs) by virtualizing these IOSs as application software [241]. This contributes to the efficiency of IOSs by making updates faster and more efficient through the use of various V2X communication modes [241]. Another way that NFV can be utilized to enhance V2X connectivity is by offloading application-level optimization activities such as load balancing to edge nodes. Additionally, several security features such as firewalls, intrusion detection systems, and virus analyzers can be generated and/or transferred between nodes on-demand, enhancing the overall security of V2X infrastructure.

However, it is essential to keep the high scalability and reliability of NFVs to ensure the reliable execution of V2X services. This is especially critical for safety-related V2X applications and services, considering the serious implications and harm to human life that a failure of such NFVs could entail. NFV and edge computing can be coupled in the future by putting selected VNFs in edge nodes for specific applications, hence improving QoS performance. VNFs can be deployed according to various factors, including computation complexity, performance criteria, and system faults. Here, machine learning methods can be utilized to forecast application or service failures or surges. This can assist in determining appropriate deployment decisions for VNFs between locations and lower expenses related to failure recovery.

### F. FEDERATED LEARNING-BASED VEHICULAR NETWORK (FLVN)

Standard machine learning techniques are often trained using data stored on a dedicated server, a cluster, or a data center [230]. Federated Learning (FL), a new mechanism for distributed machine learning, has been presented and is gaining increasing interest and appeal. FL is a machine learning method trained over several decentralized edge nodes that contain a small amount of local data without sharing it [242]. The FL framework enables vehicles to share the training operation, train their systems, and upload system parameters to the VANET infrastructure.

Federated Learning offers various performance benefits, including reduced communication overhead and higher privacy assurance, as devices do not need to share the entire dataset. Reduced communication overhead frequently leads to lower latency for training completion and reduced power consumption during communication when network capacity is limited. FL helps to identify and solve many critical issues in vehicular communications such as data security, participating privacy, data access rights, data caching, traffic prediction, data aggregation, localization accuracy, resource allocation, connected autonomous vehicles, and accessibility to heterogeneous data [243], [244], [245], [246], [247], [248], [249], [250], [251], all of which can result in improved reliability, privacy, and functionality [243], [246], [246], [247], [248], [249], [250], [251]. Using FL enables adaptation to environmental changes, such as feature learning across many geographical areas [252].

FL is a very young growing field that is still in its development cycle, with multiple outstanding issues associated with its implementation in real-time vehicular applications. Data diversity is a significant issue when applying FL to the vehicular environment. In FL, training data are stored on network edge nodes, resulting in data diversity due to the datasets' non-uniform deployment on the edge nodes. The diversity of the data introduces substantial variances into the averaged gradient data, lowering the convergence rate of learning techniques [252]. For instance, the diversity of the features on the acquired image data increases the difficulty of feature extraction and representation for NN.

Additionally, due to the large distances between vehicles, the number of edge nodes in vehicular networks is less than in conventional wireless networks. This results in model aggregation from a smaller number of edge nodes, which renders model training in VANET applications more difficult. To achieve better model training and improve the overall performance in the presence of data diversity generated by either non-uniform distribution of data or a limited number of edge nodes, one potential solution is to raise the model size, i.e., to increase the depth and width of the NN algorithm, so the NN would produce powerful feature representation [242].

However, creating wider and deeper NN models requires additional research to provide resilience in vehicular communications, which have a higher degree of data diversity than typical wireless networking systems. In this context, dataset labeling seems to be another area of research that requires additional exploration. The majority of machine learning algorithms are supervised, which means that the dataset has been labeled. Labeling data requires some work to label/annotate the gathered training data, typically done offline in existing VANET architectures. The dataset must be labeled in FL-based training so that each edge user can calculate model updates using the locally labeled dataset.

A viable solution to this challenge is to employ reinforcement learning (RL) approaches that do not involve labeled data [253]. The primary difficulty with reinforcement learning involves extended training times and typically performs worse than supervised learning due to the lack of labels. This is one of the primary difficulties associated with FL in large-scale learning-based vehicular applications. Additionally, the effectiveness of the training model is another constraint to FLVN implementation.

Transfer learning (TL)-based approaches can be used to increase the efficiency of the training model. TL is a machine learning technique in which models proposed for one task is utilized as the basis for another task [254]. It is advantageous to use TL in vehicular communications. Rather than building a model from the start, for example, a well-trained model with a big dataset can be utilized with a smooth parameter update on smaller datasets.

In this situation, the parameter updating is simplified because just a tiny section of the NN is trained, resulting in a more efficient model and lower complexity. The use of TL in vehicular networks presents data similarity problems [252]. To be precise, the TL accuracy is highly dependent on the similarity between newly gathered data at vehicular edge nodes and the training data applied to build the pre-trained system. As a result, there is a trade-off between dataset similarity/diversity and training complexity. The influence of data similarity/diversity on VANETs applications has received little attention.

As a result, novel methods to FL's learning-related challenges must be explored to make it more practical in vehicular network applications. On the other hand, communication-related issues for FL have lately garnered substantial attention for conventional wireless infrastructures that possess a high number of nodes but relatively limited node mobility [247]. Furthermore, this existing research focuses on applications with no practical relevance in the VANET domain and are tailored to traditional wireless networks' network topology and dynamics.

In this context, in comparison to centralized ml algorithms, FL enables minimizing transmission overhead through substituting model update parameter communication for raw data transfer. The model update parameter set, on the other hand, is dependent on the size of the learning model. Thus, if the model has many learnable parameters, the transmission of model parameters may create a bottleneck. Even with the reduction in transmission overhead, successfully training models over VANET communications using FL remains challenging due to the dynamic nature of the communication channel in the vehicular network due to high vehicle mobility and widely different weather conditions, resulting in frequent drop-outs and hand-overs.

Additionally, reducing transmission overhead comes at the expense of higher computing overhead at vehicle edge nodes: The edge nodes should compute gradients, which normally require powerful processors to ensure that the computation is completed and the update is transmitted on time [244], [247]. Therefore, the alternative is to either decrease the transmission overhead or improve the channel's reliability. For instance, compressed sensing and model compression are two methods for decreasing the transmission overhead in an FL-based architecture.

Besides, channel reliability could be enhanced to expedite convergence to a more suitable model. The advancement of context-aware heterogeneous infrastructures that combine the advantages of multiple wireless access technologies, for example, selecting between IEEE 802.11p, mm-wave, and VLC based on road/channel scenarios, is an exciting future research direction for significantly increasing network reliability of FL-based VANET networks. Notably, the FL model might result in an increase in network latency. The convergence rate of the model is a key metric for the rapid and accurate implementation of FL-based systems [242]. The impacts of frequent and extreme changes in VANET on FL in vehicular networks require further investigation.

Conversely, the effectiveness of scheduling and resource allocation models on FLVN has a significant impact on total system performance. Due to device heterogeneity and spatial distribution, the accessibility of wireless communication resources and the packet error rate of each node in a VANET vary significantly between vehicles [250]. Due to the fact that the rate of FL convergence is related to the function of the communications network between each edge node and the central FL controller, the scheduling and resource control of nodes participating in an FL system must be explicitly improved with the aim of optimizing the rate of FL convergence. So, more study on scheduling and resource management strategies for FLVN is required, with a high emphasis on the sparse/high-mobility network scenario.

Furthermore, data security and privacy vulnerabilities might result in poor performance and serious accidents in FLVN. Various types of devices may be used during the learning stage of FL training. Thus, unauthorized devices can more easily access the network, posing security and privacy concerns [245], [246]. Security/privacy can be accomplished through the implementation of reputation management (reward and punishment) techniques. Moreover, multiple access points functioning as servers in FL are possible in a realistic vehicular network situation, adding to the complexity of the reputation management challenge. As a result, their implementation in VANETs networks necessitates additional research into multi-server FL designs.

### G. BRAIN-CONTROLLED VEHICLE-BASED VANETS

BCV allows vehicles to be controlled by the human brain rather than by physical interaction between the vehicle and the driver. This is accomplished by involving a brain-computer interface (BCI) that can convert brain function signals to motion instructions. BCVs have considerable promise to increase flexibility and enhance the quality of life for people with disabilities by providing an alternate interface for controlling vehicles [255]. While the current ambition is for completely automated vehicles, people's adaptation will be critical for managing the unpredictability and complexity inherent in autonomous vehicles [256]. BCV aims to minimize the limits of autonomous vehicles in complex and unexpected conditions such as isolated and unstructured areas by keeping humans in the loop. in the current literature review, brain signal patterns have been used widely to operate BCV applications. Predicting a driver's desire to use emergency braking is difficult in real situations, when tension, exhaustion, cognitive load, various emotions, and external noise are all available and differ. The second limitation in BCV applications, particularly in emergency braking using physiological signals, is response time. The challenge is how often time is required to avoid a collision between vehicles traveling at various speeds; this field needs further examination.

Technically, present wireless access technologies and computational capabilities are inadequate for implementing BCV, as services requiring brain-machine interactions would require extremely high reliability, low latency, ultra-high throughput, and ultra-high-speed computing abilities. For instance, a rough guess of the need for whole-brain recording is approximately 100 Gbps [257], which cannot be transmitted using current wireless technologies. Moreover, future wireless generations should empower human drivers to learn and modify their behavior using composed entirely brain-vehicle interface and machine learning algorithms.

Also, decreasing the latency of time-consuming strategies in real-time VANETs while maintaining better accuracy and stability is another topic worth investigating. The answer is to merge the BCV with new technologies enabled by 5G/6G, which have the ability to considerably improve the quality of communication with nearly no delay, similar to real-time processing [258]. High-speed communications allow BCB based VANET services to transfer a large amount of data into cloud/edge systems for storage and processing under time limitations. Until now, there have been high demands to make studies to analyze and model the applicability of 5G/6G with BCV in different real-time VANET situations. THz networking may be a viable option for enabling high-throughput and low-delay brain-vehicle communication.

Further, reliability and cybersecurity are significant issues in BCV [258], a considerable research investigation area. Security analyses should take into account two considerations: the system security regarding hacker attacks and the system security in the event of a problem during application control. The invention of precise methods for warning the user when their focus decreases is a high priority in future literature [258]. If a disabled driver wishes to utilize a BCI framework as a carrier, they must focus for an extended time, such as eight hours. As a result, an effective alerting mechanism is necessary to assess the driver's feelings while performing tasks, such as alpha wave monitoring, eye tracking, and video processing, to tell the drivers about their current conditions and proceed with the job.

A completely novel performance measurement called quality of physical experience (QoPE) must be established and quantified to obtain physiological responses and link them to standard wireless QoS metrics [259]. BCV's feasibility has been proved in recent studies. For instance, the authors in [260], [262], and [263] demonstrated a vehicle destination selection platform based on a brain-computer interaction. Even though the BCV has been successfully launched under various settings, it is not a scalable solution because it would require wireless connectivity to allow brain-machine interfacing with high coverage, accessibility, throughput, and low latency to ensure that it is possible end-user reliability and safety. Various relevant studies are necessary to demonstrate the efficacy of BCVs, as the majority of previous research on BCVs has been validated solely through simulation. As a result, significant real-world tests are necessary to establish the efficacy of BCVs [258], [259].

### H. GREEN VEHICULAR NETWORKS

Along with these numerous benefits, the VANET presents several concerns, one of which is the negative influence on people and the surrounding landscape. The energy-intensive system increased greenhouse gas emissions, which have a detrimental effect on human health and the environment [259]. For this purpose, the growing need for innovative and pervasive applications over the last few years has shifted the vehicular networks away from self-organizing networks and toward self-sustaining networks (SSNs). One primary objective of SSNs is to minimize the necessity of independent charging of heterogeneous systems through energy-efficient communication, energy harvesting/power transfer mechanisms, and offloading of energy-intensive computing from edge devices to edge and cloud platforms. Therefore, end-users should experience the coexistence of wireless communication and power transfer mechanisms as seamlessly as possible.

Additionally, one of the primary problems is ensuring network sustainability and offering energy-efficient, energy-aware, and environment-aware vehicular connectivity to a large number of nodes and users with varying degrees of computational resources. The energy efficiency of the 6G-enabled IoV system will be crucial. Firstly, the growing number of connected IoV nodes, the associated thorough communication and computation demands, and the increasing energy need associated with the adoption of bandwidths in 6G will result in a dramatic increase in energy costs in forthcoming IoV contexts. Secondly, the cost of electricity for IoV systems and vehicle fuel emissions will increase the energy demand on the IoV infrastructure, making it more difficult to establish a sustainable VANET networking and communication infrastructure. Thirdly, the high QoS requirements and complicated, intelligent decision procedures based on big data analysis and artificial intelligence in upcoming 5G/6G-enabled V2X applications would result in significant energy consumption, creating new challenges to energy efficiency improvements [264].

Numerous studies have been conducted to implement energy-efficient vehicle networks. So, to maximize energy efficiency in next-generation V2X communications, researchers must spend extensive efforts to optimize channel allocation and communication link selection [265], [266], [267]. Several studies have been undertaken to improve offloading decisions, load distribution, and resource allocations in-vehicle edge computing contexts [268], [269], [270].

Unfortunately, these studies focus exclusively on the energy efficiency of a specific VANET scenario, omitting a full evaluation of the overall vehicular system's energy usage. Additionally, the Green Vehicle Routing Problem (GVRP) has been recognized as an essential item on the agenda in sustainability practices, gaining researchers' interest. The majority of current research on GVRP is focused on statically determined networks [271]. Thus, future research can focus on GVRP in a dynamic and changing environment (e.g., VANET) to strengthen the research's credibility.

Nevertheless, by integrating machine learning approaches with global vehicular mobility parameters (i.e., location, speed, and direction) accessible via vehicular hello packets, the compatibility time of available routes may be estimated and analyzed. This enables vehicles to estimate or forecast the compatibility time of all possible routes and then choose the optimal driving path based on the estimation results.

By utilizing renewable energy, the development of electric vehicles and hybrid electric vehicles can help reduce Green House Gas (GHG) emissions, making the deployment of VANETs more acceptable by healthcare and environmental management agencies. How to address these complexities in electric vehicle charging remains unanswered?

With the rise of alternative charging techniques and distributed charging situations, AI-based solutions for refining charging circuits and making real-time charging decisions are promising for future EV charging possibilities. Here, implementing AI-based systems, achieving rapid convergence in a real-time scheduling scenario, and securing participants' privacy are good examples of research questions. Conversely, several wireless power transmission (WPT) techniques, such as resonant beam and radio charging, can be utilized to charge electric vehicles. Therefore, enhancing charging stability and reliability with moving EVs remains a significant design challenge. Also, costs associated with building and deploying the wireless power transmission system must be minimized.

With the combination of wired and wireless power transfer techniques and a variety of charging methods (e.g., EV-to-grid, EV-to-EV, EV-to-UAV, etc.), it becomes critical to coordinate charging schedules between different charging stations and electric vehicles. Additionally, more emphasis should be made on innovating new ways to mitigate the effects of vehicular movement on the charging efficiency in the WPT. Furthermore, to enhance the fuel efficiency of EVs, VANETs can participate here through the significant emphasis on route selection, charging station distribution, and driver behavior adjustment [272], [273], [274]. But, these studies focused exclusively on the energy efficiency of a particular VANET situation.

Also, efficient management of traffic systems can assist in decreasing the energy consumption of both driving vehicles and VANETs. For instance, choosing an appropriate driving speed will conserve energy consumed during frequently stopping/starting. To make smart managerial decisions, worldwide traffic data must be gathered and updated in real-time over a fully distributed VANET network, raising communication power consumption and operational cost.

In this regard, self-learning and adaptive update techniques based on artificial intelligence will be advantageous for establishing low-complexity intelligent traffic management [275]. But, the energy demand of these artificial intelligence-based techniques must be taken into account. AI algorithms can track dynamic energy harvesting conditions and improve network architecture in an energy-harvesting system by integrating expected future energy requirements. Finally, green VANET infrastructures will undergo rigorous criteria to conserve energy, reduce emissions, and lower environmental contamination [275]. As a result, it is required to modify the current communication mode to enhance the customer experience and reduce the energy consumed by VANET infrastructures.

### I. TACTILE VEHICULAR COMMUNICATIONS

Tactile communication is a promising technology that allows a massive change away from existing digital content-oriented communications and toward control-oriented communications by enabling real-time forwarding of tactile or physiological information (i.e., smell, touch, vibration, motion, and surface texture) [276]. By integrating sensuous human information and tactile communication with VANET, vehicle users are expected to have an interactive experience [277]. With traditional multimedia communications applications (e.g., onboard conferences, infotainment), tactile communication will help boost upcoming VANET applications such as remote driving, vehicle platooning, and driver training by leveraging the stable and accurate transfer of sensor information along with haptic knowledge about driving experience and direction.

Sharing sensory data like haptics whenever and wherever tactile communications will give drivers and passengers an unmatched travel experience in the future. Autonomous vehicles are one of the applications that Tactile communications can support. It is likely to play a significant role in future efforts to reduce traffic issues, accidents, and green VANETs [278]. Limited self-driving AVs are available in the market, but technological and standard-based constraints are dominating, due to which such types of AVs are not in regular use. However, automobile manufacturers are expecting an open market for them by 2025. AVs' complete standards with tactile communications are not finalized yet; hence, the discussion on self-driving AVs seems impractical [279], [280].

Although tactile communication has substantial opportunities, it is still in its infancy, and numerous issues remain unresolved. Tactile-based VANET solutions impose strict latency, reliability, and security requirements. To provide consistent and real-time sharing of enormous volumes of haptic information, tactile communication needs incredibly high-speed and low-latency networking. To enable timely transmission of control packets and prevent possible delays, ultra-low latency of 1 ms is necessary for tactile-based VANET communications. Additionally, ultra-high dependability and security are essential for a number of the services intended for the VANET based on tactile transmission.

On a related topic, many of the applications planned for the VANET based on tactile communication require extreme reliability and security. For example, it is implausible that a data communication fault (e.g., illegal or network-based) could arise while remotely controlling an autonomous vehicle. These strict connectivity requirements are extremely challenging to achieve in situations with considerable vehicular mobility. That's because their data demands need higher frequencies (e.g., mmWave or perhaps THz) that are not, on the other hand, reliable, particularly in high mobile VANETs scenarios [201], [281].

This motivates research toward the development of a new group of services termed highly reliable high rate low latency communications (HRLLC), which can use a hybrid of conventional 5G services such as enhanced mobile broadband (eMBB) services which neglect reliability and URLLC services which neglect data rate. Besides the difficulties above, one of the primary difficulties in implementing tactile communication in a VANET environment is collecting, storing, distributing, and delivering haptic information.

Multifunctional encoding techniques need to be designed to accommodate the many modalities (i.e., vocal, visual, and haptic) of Tactile communication information while reducing overall delay [282] . In addition, achieving the haptics challenge will indeed present multiple crucial problems, including the design of application-aware control and communication methods, the creation of human-to-machine connections for wireless haptic interactions, and the design of appropriate haptic codecs for capturing and representing haptic data, as well as the precise restructuring of collected haptic data.

Additionally, multiplexing methods that combine several modalities while adhering to the 1 ms latency requirement are required. Conversely, AI-based solutions are essential for predicting haptic information that the activities, mobility, and feedback predictions are used to reduce communication latencies and disruptions. Predictions may bridge an existing gap, for example, if the command signal about the next task is not delivered early, either because of the vehicle's movement or a communication issue. In this regard, even with the tremendous data speeds given by 5G and 6G infrastructures, the latency caused by processing tactile feedback for direct interaction and executing the prediction model introduces another obstacle [283]. While algorithms may be resource and time-intensive, they should not affect the required end-to-end delay.

Accordingly, vehicles' high dynamic and movement pose a significant barrier for tactile communication-based VANET applications that demand ultra-low delay, high dependability, and a high data transfer rate [201], [279]. A communications system that satisfies these criteria has yet to be constructed [283], [284]. Finally, SDN/NFV techniques can improve the networking domain in tactile vehicular communication [283]. Typical network techniques cannot implement QoS control efficiently or adapt to rapidly changing network operations.

The discovery of innovative SDN strategies in conjunction with NFV can assist in resolving this issue. Additionally, there is a high demand for innovative architectures which go beyond offloading and executing modules on MEC nodes, as such techniques have shown inconsistent outcomes.

### J. QUANTUM COMPUTING AIDED VANET

In comparison to 5G-based V2X, future V2X is predicted to handle a greater spectrum, a massive number of densely linked vehicles, a broader range of applications, a higher degree of signal complexity, and more strict criteria for reliability, latency, and power economy. To achieve these needs, the next generation of V2X systems will require significantly more computational power than is now available. These resources are needed to implement many computationally intensive actions in a timely manner.

With the arrival of quantum computing, wireless communication will have a significantly improved computational dimension, enabling the ultra-fast implementation of highly complicated algorithms, particularly signal processing tasks that cannot be executed in real-time with regular computational resources.

For instance, implementing complex deep learning algorithms that require big data processing and huge training (e.g., determining the optimal geographic route for many purposes) is a difficult undertaking. In these cases, classical computing frequently makes a trade-off between efficiency and complexity, but quantum computing, on the other side, can effectively attain optimal solutions with lower complexity [285], [286].

Along with greater computational capability, quantum computing improves the security of wireless communications [285]. Take note that security is substantially more critical in V2X communications than in regular communications, as a security vulnerability in autonomous vehicles, for example, can result in deadly accidents. In this regard, to sharing of the wireless spectrum by vehicles and other types of network nodes (e.g., passengers' handhelds), V2X communications may be subject to hostile attacks, and typical encryption techniques may be insufficient. Quantum computing incorporates the underlying security feature of quantum theory, which cannot be duplicated or obtained without interfering with it [287], making it an ideal tool for enhancing the security of 6G-V2X communications.

Meanwhile, quantum algorithm methods have gained great advances in recent years. As shown in a study published by the National Institute of Standards and Technology (NIST) [288], existing cryptographic techniques require larger key sizes. NIST specifically advised against using integer factorization-based cryptographic methods, stating that RSA and ECC are no longer reliable in quantum computing. As a result, once a quantum computer is introduced, all existing V2X communication protocols will be rendered obsolete, posing both safety and privacy risks [289].

While quantum computing has the potential to be an emerging tool for 6G-V2X communication from a variety of perspectives, many more studies are required to fully utilize and apply the capabilities of quantum computing in data transmission. For instance, present quantum computer chips can work at freezing temperatures (near zero Kelvin), limiting their application to VANET infrastructure. Significant research on the heat stability of quantum computer chips is required before they may be used in vehicles. Additional basic difficulties include the creation of large-scale quantum computing, the development of quantum security infra-architectures, and the measurement of quantum spreading. The commercialization of self-driving vehicles is predicted to change in the short term [290]. Accordingly, recent reports have shown that quantum computing is expected to reach commercialization faster than autonomous driving [291], [292], [293].

### K. MULTI-RADIO ACCESS V2X NETWORKS

Utilizing the higher spectral bands such as mmWave and THz range is critical for addressing the demand of the next generation of V2X applications, which include Tbps data speeds, millions of connected nodes, and latency of less than a millisecond. The extensive frequencies in the mmWave and THz bands enable the provision of more bandwidth near to multi-Gigabits than the sub-6 GHz band, which is suffered from extreme congestion in the cellular networks [277].

This extraordinary throughput enables dozens of novel V2X applications, for example, ultra-fast huge data transmission between vehicles and tactile interfaces. THz communication can be utilized in on-board using cases such as the BCV situation that requires exceptionally high data rates and low latency [82], [83], [154] , [201]. Besides, V2X communications in the mmWave and THz radio frequencies undergo high propagation losses and are susceptible to blocking by barriers like automobiles and constructions [82], [83], [154], [281]. Additionally, the much smaller cells in the mmWave and THz communications may significantly increase handover frequencies. These issues make it difficult for mmWave and THz communications to deliver the required QoS for emerging V2X scenarios [281].

Multi-radio access methods operating at sub-6 GHz, mmWave, and THz are expected to coexist in future V2X infrastructures [294]. Whereas mmWave and THz communications will add capacity and bandwidth to V2X infrastructure, sub-6 GHz radios are crucial for long communication ranges and connections reliability. There is a range of issues that must be addressed in order to maximize the efficiency of multi-radio access VANET networks.

The significant transmission loss and signal blocking in mmWave/THz-based V2X communications require directional beamforming. Unfortunately, the difficulties introduced by mmWave and THz at the MAC layer due to beamforming communications are still unresolved for V2V communications. Innovative mechanisms for coordination and collaboration of multi-radio access networks are required to address MAC layer issues such as rapid link configuration and beam maintenance, distributed congestion control, contention-based channel access, side-link automatic scheduling, and interference administration.

Also, other major issues need to be resolved, including transceiver systems, antenna design adaptability, propagation characterization, channel analysis, and the integration of new communication modes. It is critical to analyze and interpret the radio propagation of these bands in a variety of V2X situations, including highway, rural, and OBU-vehicle.

One of the primary issues in multi-radio-aided V2X will be maximizing the usage of existing cellular networks [277], [294]. So, appropriate intelligent resource scheduling is essential to use their specific advantages. For instance, whereas THz networking allows high data transfer rates, it is mainly suited for short-range V2X data transmission. In this scenario, resources could be assigned in bands to transmitters with short-range receivers. To solve the issues associated with multi-radio systems and increased computational complexity, innovative resource allocation systems are required that may be constructed with situational awareness and cross-layer architecture.

A multimodal spectrum management paradigm can be developed in which connected vehicles are provided with both reserved radio resources and a shared resource pool supporting V2V and V2I interactions. The allocation could be changed dynamically in response to QoS feedback and situational factors.

Situational awareness of the VANET network and the driving system may be critical for developing cross-layer solutions for spectrum utilization. Additionally, the high mobility nature of VANET networks and the restrictive QoS demands required to maintain highly developed V2X use cases complicate the radio resource management problems. To address the massive action space and time variability of radio resource management and QoS control issues, distributed AI-based techniques across multiple radios capable of adaptively allocating resource blocks and power must be planned. Such intelligent alternatives could be designed via reinforcement learning.

### L. VLC-ASSISTED V2X SYSTEM

Next-generation of VANETs intends to feed vehicle drivers and passengers with services at exceptionally high data speeds and incredibly low latency in the future V2X. This functionality, however, may not be possible with conventional RF-based vehicular communications that generally suffer from severe interference, high latency, and low network throughput rates in dense areas [171]. One solution is to combine Radiofrequency and visible light communication (VLC) in V2X communications, in which visible light can be used in conjunction with radio waves to communicate in V2X networks. VLC technology is a perfect choice for upcoming ITS where the ultra-high data rate is achieved by light-emitting diode (LED) or laser diode (LD)-based VLC, low energy requirements, improved security, and minimized electromagnetic interference make it a perfect candidate [294].

Additionally, VLC-enabled V2X communications have a low setup cost since they can be deployed using available LEDs/LDs in vehicle lights or pre-existing traffic lights. VLC is primarily utilized in three cases in V2X networks: V2V connectivity using headlights and backlights, V2X connectivity through traffic lights, and V2X connectivity through streetlamps. Notably, traffic or street lights can be utilized to form backhaul connections between themselves using free-space coherent optical communication [259].

Along with increasing data rates, VLC can improve the performance of V2X infrastructure by removing the constraints associated with conventional RF-based V2X communications. For instance, when large vehicle shadowing occurs, RF-enable vehicular communication suffers from substantial packet loss due to packet collision and high path loss [295]. In this case, the sending vehicle can interact with the large vehicle via VLC, and the large vehicle can then pass the data to the vehicles in the shadow area. Likewise, traffic lights can be used to relay packets between vehicles traveling on opposite roads, where traditional RF-enabled V2V communication may suffer from substantial link failure.

While RF-based solutions to the challenges mentioned above have been examined in the literature, such systems can introduce significant interference in high-density scenarios due to RF-based re-transmissions [296]. Though substantial research on VLC-enabled VANET has been conducted over the last decade, VLC is not modeled and analyzed in the 5G/6G-V2X technology. Numerous outstanding difficulties must be resolved before hybrid RF-VLC V2X may be enabled, including interoperability challenges between VLC and RF systems and deployment concerns.

VLC's performance declines in an outdoor environment because of interference from natural and installed light sources. Conversely, the received signal intensity in VLC can vary significantly due to the motion of the vehicles [297], [298]. Thus, interference caused by ambient lighting and signal fluctuations caused by mobility must be handled correctly before introducing VLC in V2X networks.

### M. INTEGRATED LOCALIZATION AND COMMUNICATION

Acquiring exact vehicle position information in real-time is progressively essential, not just for exploring the limitless possibilities of location-based applications but also for innovative V2X solutions such as real-time 3D mapping for generating a precise environment model. Additionally, reliable location information increases VANET's serv-ices delivery quality. As it is planned, 6G is expected to offer a new facility to wireless communication networks termed integrated localization and communication (ILAC) [299]. Centimeter-level localization precision is envisaged in this new paradigm, which leverages ultra-massive MIMO, mmWave communication, and UAV/satellite systems.

On the other hand, the location information provided by the vehicles can help VANET infrastructure in various ways, including providing location-assisted channel state information, beam encoding, data tracking, network planning, and communication optimization, to maximize the utilization of VANET infrastructure and broadcast resources. A significant difficulty here is properly dividing radio resources between localization and communication while still meeting their QoS constraints. To address this issue, machine learning-based technologies can be applied, as such techniques can intelligently reveal the full capabilities of radio resources [299]. Another issue for ILCA is designing appropriate waveforms with ultra-high transmission rates, which efficient spectrum sharing strategies can overcome. It is also necessary to consider the unified design of transceivers to achieve complete integration of localization and communication.

### N. 6G-BASED V2X COMMUNICATION

The primary objective of building such a network is to expand the system's intelligence and the environment's adaptability for various application criteria, such as enhanced mobile broadband and URLLC. 6G is intended to provide ultra-reliable high-rate V2X communications in contexts with high mobility. Connected autonomous vehicles and high-speed trains traveling at speeds of up to 1000 km/h will connect with one another and with their environment via a variety of sensors, network nodes (e.g., RSUs, BSs, and robotics), satellites, and the network cloud. 6G enabled V2X is a hybrid space-air-ground infrastructure that interfaces more wisely with humans than any other networking system. 6G brings extraordinary data rates, and devices ought to be able to take full advantage of them.

Currently, the majority of OBUs devices are created around 4G/5G concepts, and they must be constructed in such a way that they can be utilized with 6G as well. Additionally, such devices are incapable of supporting all of 6G's unique features, including AI, augmented and virtual reality, high quality of service, autonomous vehicles, and OBUs sensing and communication [300]. However, the 6G network's key performance indicators (KPIs) require significant improvement in the areas of intelligent broadcasting, network intelligence, and self-learning with proactive analysis [285]. It is expected that the 6G-V2X networks will have huge volumes of data that have been collected and sophisticated network architectures, intro big problems for AI-driven learning and training operations. Additionally, the current computational resources may indeed be inadequate to analyze massive amounts of high-dimensional data at the required accuracy rate for training.

As a result, developing efficient intelligent systems for 6G-based VANETs that improve both processing accuracy and efficiency represents a substantial development challenge. However, even orthogonal frequency-division multiplexing (OFDM) and its derivatives are used for high-rate communications in both LTE and 5G NR are extremely vulnerable to the Doppler effect, which can undermine multi-carrier orthogonality, resulting in maximized inter-carrier and inter-symbol interference [301], [302]. To address this shortcoming, several sophisticated multicarrier waveforms may be ideal candidates for 6G-based V2X communications [303]. Orthogonal time-frequency space (OTFS) has recently developed as an efficient multi-carrier strategy for distributing each information symbol across a 2D orthogonal basis function spanning the time-frequency domain [304], [305], [306]. However, the modeling and analysis of OTFS in 6G-based V2X require more research efforts.

Additionally, current NOMA research focuses mostly on its application to huge machine-type communications with poor mobility and transmission rates. To enable ultra-reliable Super-transfer rate communication for autonomous vehicles, for example, it is, therefore, worthwhile to investigate the combination of NOMA (e.g., SCMA) and OTFS (or variants) in order to maximize the benefits of these two disruptive approaches. On the other hand, THz bands are expected to be used broadly in 6G communications. However, the limitation of THz signals transmission and low wavelength provide an additional obstacle to the applicability of THz-enabled 6G communication in high mobility and dense V2X data transmission.

As a result, the signal's range will be limited to a few meters, and it is not commercially feasible to install signal amplifiers every few meters to sidestep this limitation. If there is moisture, THz signal attenuation is amplified, thus reducing its range [307]. Meanwhile, the data transfer generated in 6G-based V2X will approach exabytes, resulting in a massive increase in the number of connected entities.

At the moment, big data techniques are capable of processing massive volumes of data from a single source, but not of processing small amounts of data from a variety of heterogeneous sources [308]. So, the existing infrastructure is incapable of handling this volume of data, and so hardware optimizations and supercomputers techniques may be required to process such data in V2X. To enable such changes, additional modifications to current big data techniques are required [308], [309]. The current technologies of data analysis and communication require more developments to allow the future vision of 6G-based VANET communications as intelligent, autonomous, user-driven communications and a platform as a service for ITS.

### O. TRUST MODEL-BASED VANET

During the last few years, various network paradigms and emerging technologies have been proposed to enhance data delivery and communication scalability in vehicular communication. Subsequently, various VANET variations have been introduced such as Vehicular Cloud (VC), C-V2X, SDVN, 5G-based VANET, UAV-assisted VANETs, and Vehicular Fog Computing (VFC) paradigms [19], [53], [84], [157], [195]. Though, these network infrastructures and technologies have been offered many benefits to VANET in terms of reliability, scalability, availability, and accessibility but the security and privacy challenges are intensively increased where there are more options and vulnerabilities to attack the system [23], [36]. They are vulnerable to various attacks and threats. These security breaches and attacks may cause adverse incidents such as road accidents and traffic jams.

To design a better security system, the threats and vulnerabilities of such architectures need to be model and evaluate comprehensively. However, threat modeling can provide a systematic and proactive methodology to study and examine all the phases of security, threats, and vulnerabilities of a system independently of their seriousness and potential consequences [310]. It supports to recognize the attack vector, attacker profile, security system requirements, and the possible mitigation approaches based on the well-known security mechanisms. Such information can be utilized as a reference during the test phase to avoid omitted threats [306].

From this time, there is a high demand to develop a complete VANET-driven threat model that has the ability to provide details about the security of different VANET infrastructures. The development of these models is essential before designing security solutions. In this regard, there are some trade-offs in performance and security requirements of VANET networks. The security solution need to be compatible with VANET infrarchitecture and requirements after proper determination of security requirements of the particular VANET system. Therefore, the security solution must take into account the design and architecture of the system and meet the security requirements to mitigate unsystematic use of security mechanisms.

To develop a threat model, we must consider the system from the attacker's perspective in order to identify the most valuable assets and potential vulnerable points. Security and privacy issues of VANET architectures have not been examined widely yet [310]. Hence, the security designation and requirements are not obvious in this context.

Most of the time, the solution to a security vulnerability is developed based on intuition, brainstorming, or current attack occurrences that are not methodical approaches to addressing the security vulnerabilities. The threat model can be used to verify the assumptions from brainstorming and to support the countermeasures applied in the security solution [307]. However, there is an urgent need to develop comprehensive threat models to provide systematic approaches to design security solutions for different VANET architectures. When a system's vulnerabilities and threats are modelled properly, well-known security solutions can be defined and used to address each one of the potential security vulnerabilities. A well-defined threat model can assist to examine the security and privacy threats, vulnerabilities, requirements, and concerns along with the attacker model, the attack purposes, and attacker abilities [310], [311], [312]. Threat model analysis in different VANET infrastructures is critical where only brainstorming and threat models of other VANET network paradigms cannot cover the complete scenario of potential threats and vulnerabilities of different infrastructures.

Recently, vehicles manufacturing has changed significantly where autonomous vehicles have taken the lead in the automotive industry. This can be realized through the increased use of automotive embedded systems and the large quantity of embedded sensors and applications which are integrated within every single vehicle [69], [121]. Additionally, such vehicles are equipped with various communication technologies, such as DSRC, Wi-Fi, 5G, and Bluetooth, allowing them to cooperate and communicate with each other and with roadside units. This opens the door to different cybersecurity threats and makes the autonomous vehicle a more attractive target for attackers. For that reason, the need to develop systematic threat model to examine and ensure the security of the autonomous vehicles components and connectivity becomes critical [313]. Developing such models should include the determining of the security requirements, vulnerabilities and system threats, and the attackers who might target it. Threat modeling of autonomous vehicles helps to decrease the lifecycle and the cost of achieving security objectives when it is considered during the design process [311].

In literature there are different methods were suggested to develop threat modeling. Each of them has focused on a specific aspect of the system such as asset, attacker, software, or system vulnerabilities [311], [314]. Typically, the suggested threat modeling has been developed using one of these different methods independently. So, the question of how can these methods use in the VANET domain is still need more research work. Moreover, several of suggested trust models to improve the security in VANET did not consider a variety of behavioral conditions and unpredicted VANET situations [315].

### *P. COMPUTING EDGE-BASED VANET*

Today, AVs are an emerging research topic with high upcoming advantages for disabled and old people. AVs has a huge number of embedded sensors ranging from standard sensors system such as GPS and ultrasonic sensors to more specialized camcorders and LiDAR sensors [121]. These sensors will support to improve the vision and make decisions before access danger area alike to adaptive cruise control system and reroute assistance. However, these sensing systems generate huge quantities of data that require powerful computation resources and high data rates to be utilized. In a dense driving situation, a massive amount of sensor data (e.g. video stream and LiDAR visions) should be collected, processed, interpreted, and delivered to autonomous vehicles in very low latency [142]. Also, such vehicles are enhanced with hardware and software that can provide different entertainment and comfort applications. However, these services open up more challenges in VANET communication not only in terms of security and privacy but also in terms of reliability and QoS. In next times, the VANETs related data will be often collected from various sources and nodes [316]. This data is used for different purposes such as data routing, broadening the driver awareness, predicting vehicles mobility, improving passenger comfort, safety applications, and quality of road experience. Using AI algorithms in VANET application domains can enhance the network performance and data reliability. Due to its remarkable problem-solving capabilities and high ability to enhance conventional data-driven methods, AI algorithms can provide AVs with promising models for the environment awareness and sufficient decision-making for smooth navigation [317]. In general, AI algorithms have higher computation overheads and resource requirements. The vehicles resources and local RSUs may be insufficient to implement AI models within minimum latency. Thus, the integration of emerging architectures and access technologies such as fog and edge computing can help in alleviate the computation burden of AI based solutions by migrating part or all of the computations from vehicles to external computation systems and storage servers founded at the edge, fog, or cloud [318]. The limitations of the network connectivity to cloud servers prevents some types of applications, such as those requiring ultra-low-latency or high bandwidth. Accordingly, the modern VANET architectures involve edge-cloud technologies where there will be three layers [317]. The first layer includes vehicles nodes, the second layer is edge cloud layer, and traditional cloud services at layer three. Edge cloud helps to solving the problems of latency and bandwidth and when integrated with 5G/6G systems, will provide new forms of services that cannot be achieved properly with traditional cloud, such as cooperative environment perception. Edge computing technology helps to provide context aware storage and distributed computing near data sources providing ultra-low-latency communications with high bandwidth to the end user [240]. A well-trained ML learning model can be achieved on cloud or edge servers for inference [319]. The utilization of the high computational nodes (e.g. MEC servers) in the deployment of the trained learning model will be very useful for attaining efficiency in the autonomous field. However, even with the great advantages of edge-cloud VANET architecture but there are many challenges and issues that need to be addressed properly. Edge cloud nodes localization and performance measurement are not examined comprehensively in real-time environment yet. Also, High vehicles mobility leads to delay increasing as vehicles travel out the communication range of the edge cloud resides. The measurement of vehicles mobility on the performance of edge computing nodes requires more research attention. Additional challenges concern the ability to decide and then choose an edge cloud that is available and suitable in terms of performance and communication reliability, and orchestrate that choice over the whole road trip with consistent migration of applications among edge clouds. Also, one of the main challenges here is the ability to distribute applications and computation burden across layers (local, edge cloud, and core cloud) and to decide the suitable division of an application across multiple layers and nodes and control that division as resources change without noticeable reduction in QoS and QoE, is desirable to realize the future of VANETs. In this context, awareness of the present level of functionality and computation load at each layer, which will change as the VANET nodes change, is essential to allow changes in the distribution as required. Consequently, reliable solutions to measure QoS and predict changes in performance can be helpful in the initiation of alternate configuration proactively when the undesirable drop in overall performance is reached.

## VIII. CONCLUSION

VANET network helps to improve human safety against road collisions and optimizes road transportation management. To present, a substantial quantity of studies has been conducted to survey solutions for different challenges and issues of vehicular networks such as routing, security, and communication improvement. Nevertheless, a whole work to review vehicular networks from various aspects such as communications, applications, and challenges are still missing. Therefore, this paper presents a comprehensive survey on the available wireless access technologies that can be applied to VANETs.

A widespread description of the VANET services has been provided with more clarifications about its classification explicitly from their usability and applicability to safety-related, infotainment, transportation traffic improvement, and driving system monitoring applications. Also, the challenges and issues of a vehicular infrastructure are studied and organized obviously from the perspective of applications (safety-related applications challenges, traffic management applications challenges, non-safety-related applications challenges), data networking (data routing, data security, data dissemination), and VANET resources management (radio resources allocation challenges, VANET infrastructure deployment challenges, C-V2X challenges).

Furthermore, the future difficulties and research areas that will assist academia and industrial companies in developing novel techniques and solutions by integrating cutting-edge technologies and networking infrastructure to achieve the ITS purpose collaboratively and fully automated transportation systems are detailed comprehensively. Besides, the imperfections and leaks in the application of different new emerging technologies in VANET communication such as federated learning, VLC, and 6G are clarified. Integration of VANET with other enabling paradigms such as IoT, VNF, tactile communications, and quantum technologies is essential to support the new services and applications in upcoming V2X communication and therefore the challenges of such integrations have been addressed obviously in this work. Also, the new proposals and solutions to integrating such technologies with vehicular networks are presented here.

However, according to the findings and study, while VANET offers tremendous promise in modern transportation systems, there are various challenges that must be addressed. It has applications in a variety of sectors, including safety, traffic safety, comfort and infotainment, and healthcare, but its applicability and incorporation in more areas must be enhanced. Overall, reviewing a vehicular network from different aspects shows that one size fits all' ideas can realize, allowing readers and researchers to find all things in one box while encouraging and inspiring further researchers to this interesting area of research.

## REFERENCES

[1] S. Sharma and B. Kaushik, "A survey on Internet of Vehicles: Applications, security issues and solutions," *Veh. Commun.*, vol. 20, Dec. 2019, Art. no. 100182, doi: 10.1016/j.vehcom.2019.100182.

[2] M. Lee and T. Atkison, "VANET applications: Past, present, and future," *Veh. Commun.*, vol. 1, Apr. 2020, Art. no. 100310, doi: 10.1016/j.vehcom.2020.100310.

[3] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad-hoc network," *J. Netw. Comput. Appl.*, vol. 37, pp. 380–392, Jan. 2014.
[4] C. Campolo, H. A. Cozzetti, A. Molinaro, and R. Scopigno, "Augmenting vehicle-to-roadside connectivity in multi-channel vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 36, no. 5, pp. 1275–1286, Sep. 2013.
[5] C. Lai, D. Zheng, Q. Zhao, and X. Jiang, "SEGM: A secure group management framework in integrated VANET-cellular networks," *Veh. Commun.*, vol. 11, pp. 33–45, Jan. 2018.
[6] A. Bazzi, B. M. Masini, A. Zanella, C. De Castro, C. Raffaelli, and O. Andrisano, "Cellular aided vehicular named data networking," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Nov. 2014, pp. 747–752.
[7] B. Aslam, P. Wang, and C. C. Zou, "Extension of Internet access to VANET via satellite receive-only terminals," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 14, no. 3, pp. 172–190, 2013.
[8] B. Kloiber, T. Strang, H. Spijker, and G. Heijenk, "Improving information dissemination in sparse vehicular networks by adding satellite communication," in *Proc. IEEE Intell. Vehicles Symp.*, Jun. 2012, pp. 611–617.
[9] A. Kumar and S. Niwashn, "Implementation of VANET in transportation using wireless sensors," *Int. J. Sci. Res. Eng. Technol.*, vol. 4, no. 6, p. 2278, 2015.
[10] J. M.-Y. Lim, Y. C. Chang, M. Y. Alias, and J. Loo, "Cognitive radio network in vehicular ad hoc network (VANET): A survey," *Cogent Eng.*, vol. 3, no. 1, Dec. 2016, Art. no. 1191114.
[11] K. D. Singh, P. Rawat, and J. M. Bonnin, "Cognitive radio for vehicular ad-hoc networks (CR-VANETs): Approaches and challenges," *EURASIP J. wireless Commun. Netw.*, vol. 2014, no. 1, pp. 1–22, 2014
[12] R. Li and P. Zhu, "Spectrum allocation strategies based on QoS in cognitive vehicle networks," *IEEE Access*, vol. 8, pp. 99922–99933, 2020, doi: 10.1109/ACCESS.2020.2997936.
[13] M. A. Al-Absi, A. A. Al-Absi, M. Sain, and H. Lee, "Moving ad hoc networks—A comparative study," *Sustainability*, vol. 13, no. 11, p. 6187, May 2021, doi: 10.3390/su13116187.
[14] A. Srivastava and J. Prakash, "Future FANET with application and enabling techniques: Anatomization and sustainability issues," *Comput. Sci. Rev.*, vol. 39, Feb. 2021, Art. no. 100359.
[15] O. S. Oubbati, M. Atiquzzaman, P. Lorenz, M. H. Tareque, and M. S. Hossain, "Routing in flying ad hoc networks: Survey, constraints, and future challenge perspectives," *IEEE Access*, vol. 7, pp. 81057–81105, 2019.
[16] S. Jiang, Z. Huang, and Y. Ji, "Adaptive UAV-assisted geographic routing with Q-learning in VANET," *IEEE Commun. Lett.*, vol. 25, no. 4, pp. 1358–1362, Apr. 2021.
[17] R. A. Nazib and S. Moh, "Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: A survey," *IEEE Access*, vol. 8, pp. 77535–77560, 2020, doi: 10.1109/ACCESS.2020.2989790.
[18] B. Hament and P. Oh, "Unmanned aerial and ground vehicle (UAV-UGV) system prototype for civil infrastructure missions," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2018, pp. 1–4.
[19] S. Sharma and A. Kaul, "VANETs cloud: Architecture, applications, challenges, and issues," *Arch. Comput. Methods Eng.*, vol. 28, no. 4, pp. 2081–2102, Jun. 2021.
[20] P. Shah and T. Kasbe, "A review on specification evaluation of broadcasting routing protocols in VANET," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100418.
[21] S. Khatri, H. Vachhani, S. Shah, J. Bhatia, M. Chaturvedi, S. Tanwar, and N. Kumar, "Machine learning models and techniques for VANET based traffic management: Implementation issues and challenges," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 3, pp. 1778–1805, May 2021.
[22] A. Mchergui, T. Moulahi, and S. Zeadally, "Survey on artificial intelligence (AI) techniques for vehicular ad-hoc networks (VANETs)," *Veh. Commun.*, vol. 34, Apr. 2022, Art. no. 100403.
[23] R. Hemalatha, "A survey: Security challenges of vanet and their current solution," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 2, pp. 1239–1244, Apr. 2021.
[24] K. H. Rashmi and R. Patil, "Survey on cross layer approach for robust communication in VANET," *Wireless Pers. Commun.*, vol. 119, no. 4, pp. 3413–3434, Aug. 2021.
[25] H. A. Ameen, A. K. Mahamad, S. Saon, D. Md Nor, and K. Ghazi, "A review on vehicle to vehicle communication system applications," *Indonesian J. Elect. Eng. Comput. Sci.*, vol. 18, no. 1, pp. 188–198, 2020.
[26] D. Manivannan, S. S. Moni, and S. Zeadally, "Secure authentication and privacy-preserving techniques in vehicular ad-hoc NETworks (VANETs)," *Veh. Commun.*, vol. 25, Oct. 2020, Art. no. 100247.
[27] A. Srivastava, A. Prakash, and R. Tripathi, "Location based routing protocols in VANET: Issues and existing solutions," *Veh. Commun.*, vol. 23, Jun. 2020, Art. no. 100231.
[28] O. S. Al-Heety, Z. Zakaria, M. Ismail, M. M. Shakir, S. Alani, and H. Alsariera, "A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET," *IEEE Access*, vol. 8, pp. 91028–91047, 2020.
[29] S. Raza, S. Wang, M. Ahmed, and M. R. Anwar, "A survey on vehicular edge computing: Architecture, applications, technical issues, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–19, Feb. 2019.
[30] R. Gasmi and M. Aliouat, "Vehicular ad hoc NETworks versus Internet of Vehicles—A comparative view," in *Proc. Int. Conf. Netw. Adv. Syst. (ICNAS)*, Jun. 2019, pp. 1–6.
[31] A. Singh, L. Gaba, and A. Sharma, "Internet of vehicles: Proposed architecture, network models, open issues and challenges," in *Proc. Amity Int. Conf. Artif. Intell. (AICAI)*, Feb. 2019, pp. 632–636.
[32] A. Benmir, A. Korichi, A. Bourouis, and M. Alreshoodi, "Survey on QoE/QoS correlation models for video streaming over vehicular ad-hoc networks," *J. Comput. Inf. Technol.*, vol. 26, no. 4, pp. 267–287, 2018.
[33] A. Zekri and W. Jia, "Heterogeneous vehicular communications: A comprehensive study," *Ad Hoc Netw.*, vols. 75–76, pp. 52–79, Jun. 2018.
[34] P. Mutalik and V. C. Patil, "A survey on vehicular ad-hoc network [VANET's] protocols for improving safety in urban cities," in *Proc. Int. Conf. Smart Technol. For Smart Nation (SmartTechCon)*, Aug. 2017, pp. 840–845.
[35] A. Mchergui, T. Moulahi, B. Alaya, and S. Nasri, "A survey and comparative study of QoS aware broadcasting techniques in VANET," *Telecommun. Syst.*, vol. 66, no. 2, pp. 253–281, Oct. 2017.
[36] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "VANet security challenges and solutions: A survey," *Veh. Commun.*, vol. 7, pp. 7–20, Jan. 2017.
[37] S. Ilarri, T. Delot, and R. Trillo-Lado, "A data management perspective on vehicular networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2420–2460, 2015.
[38] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, "Heterogeneous vehicular networking: A survey on architecture, challenges, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2377–2396, 2015.
[39] M. Chaqfeh, A. Lakas, and I. Jawhar, "A survey on data dissemination in vehicular ad-hoc networks," *Veh. Commun.*, vol. 1, no. 4, pp. 214–225, 2014.
[40] A. Haydari and Y. Yilmaz, "Deep reinforcement learning for intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 1, pp. 11–32, Jan. 2020.
[41] I. Laña, J. J. Sanchez-Medina, E. I. Vlahogianni, and J. Del Ser, "From data to actions in intelligent transportation systems: A prescription of functional requirements for model actionability," *Sensors*, vol. 21, no. 4, p. 1121, Feb. 2021.
[42] A. Paul, N. Chilamkurti, A. Daniel, and S. Rho, *Intelligent Vehicular Networks and Communications: Fundamentals, Architectures and Solutions*. Amsterdam, The Netherlands: Elsevier, 2016.
[43] A. Richter, M.-O. Löwner, R. Ebendt, and M. Scholz, "Towards an integrated urban development considering novel intelligent transportation systems," *Technol. Forecasting Social Change*, vol. 155, Jun. 2020, Art. no. 119970.
[44] M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," *Wireless Commun. Mobile Comput.*, vol. 2019, pp. 1–23, Sep. 2019.
[45] (2016). Organisation Internationale des Constructeurs d'Automobiles (OICA). *Number of Passenger Cars and Commercial Vehicles in use Worldwide From 2006 to 2014 in (1,000 Units) 2014*. Accessed: Jan. 19, 2022. [Online]. Available: http://www.statista.com/statistics/281134/number-of-vehicles-in-useworldwide/
[46] F. B. S. D. Carvalho, W. T. A. Lopes, M. S. Alencar, and J. V. S. Filho, "Cognitive vehicular networks: An overview," *Proc. Comput. Sci.*, vol. 65, pp. 107–114, Jan. 2015.
[47] A. Daniel, A. Paul, A. Ahmad, and S. Rho, "Cooperative intelligence of vehicles for intelligent transportation systems (ITS)," *Wireless Pers. Commun.*, vol. 87, no. 2, pp. 461–484, Mar. 2016.

[48] S. Temel, M. C. Vuran, M. M. R. Lunar, R. K. Faller, and C. Stolle, "Vehicle-to-barrier communication during real-world vehicle crash tests," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Dec. 2016, pp. 1–8.

[49] S. Rangarajan, M. Verma, A. Kannan, A. Sharma, and I. Schoen, "V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning," in *Proc. Int. Conf. Adv. Comput., Commun. Informat. (ICACCI)*, 2012, pp. 148–154.

[50] L. Liang, H. Ye, and G. Y. Li, "Towards intelligent vehicular networks: A machine learning framework," *IEEE Internet Things J.*, vol. 1, no. 9, pp. 2581–5782, Sep. 2018.

[51] E. Schoch, F. Kargl, M. Weber, and T. Leinmuller, "Communication patterns in VANETs," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 119–125, Nov. 2008.

[52] M. D. Nuri and H. H. Nuri, "Strategy for efficient routing in VANET," in *Proc. IEEE Int. Symp. Inf. Technol. (ITSim)*, vol. 2, Jun. 2010, pp. 903–908.

[53] A. Ullah, X. Yao, S. Shaheen, and H. Ning, "Advances in position based routing towards ITS enabled FoG-oriented VANET—A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 2, pp. 828–840, Feb. 2020.

[54] 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, Apr. 2014.

[55] Y. Sasaki, W.-C. Lee, T. Hara, and S. Nishio, "On alleviating beacon overhead in routing protocols for urban VANETs," in *Proc. IEEE 14th Int. Conf. Mobile Data Manage. (MDM)*, vol. 1, Jun. 2013, pp. 66–76.

[56] W. Qi, Q. Song, X. Wang, L. Guo, and Z. Ning, "SDN-enabled social-aware clustering in 5G-VANET systems," *IEEE Access*, vol. 6, pp. 28213–28224, 2018.

[57] D. Shukla, A. Prakash, and R. Tripath, "Comparative analysis of channel estimation techniques in vehicular communication," in *Advances in VLSI, Communication, and Signal Processing*. Singapore: Springer, 2021, pp. 679–688.

[58] F. Li, W. Chen, and Y. Shui, "Study on connectivity probability of VANETs under adverse weather conditions at 5.9 GHz," *IEEE Access*, vol. 8, pp. 547–555, 2020, doi: 10.1109/ACCESS.2019.2962089.

[59] J. Liu, J. Wan, Q. Wang, P. Deng, K. Zhou, and Y. Qiao, "A survey on position-based routing for vehicular ad-hoc networks," *Telecommun. Syst.*, vol. 62, no. 1, pp. 15–30, May 2016.

[60] J. B. P. Neto, L. C. Gomes, F. M. Ortiz, T. T. Almeida, M. E. M. Campista, L. H. M. K. Costa, and N. Mitton, "An accurate cooperative positioning system for vehicular safety applications," *Comput. Electr. Eng.*, vol. 83, May 2020, Art. no. 106591.

[61] Y. Sun, L. Wu, S. Wu, S. Li, T. Zhang, L. Zhang, J. Xu, Y. Xiong, and X. Cui, "Attacks and countermeasures in the Internet of vehicles," *Ann. Telecommun.*, vol. 72, nos. 5–6, pp. 283–295, Jun. 2017.

[62] H. Aouzellag, K. Ghedamsi, and D. Aouzellag, "Energy management and fault tolerant control strategies for fuel cell/ultra-capacitor hybrid electric vehicles to enhance autonomy, efficiency and life time of the fuel cell system," *Int. J. Hydrogen Energy*, vol. 40, no. 22, pp. 7204–7213, Jun. 2015.

[63] B. Alaya and L. Sellami, "Clustering method and symmetric/asymmetric cryptography scheme adapted to securing urban VANET networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102779.

[64] G. Abdelkader, K. Elgazzar, and A. Khamis, "Connected vehicles: Technology review, state of the art, challenges and opportunities," *Sensors*, vol. 21, no. 22, p. 7712, Nov. 2021.

[65] V. Malik and S. Bishnoi, "Security threats in VANETS: A review," *Int. J. Recent Res. Aspects*, vol. 2, pp. 72–77, Mar. 2014.

[66] B. Ji, X. Zhang, S. Mumtaz, C. Han, C. Li, H. Wen, and D. Wang, "Survey on the Internet of vehicles: Network architectures and applications," *IEEE Commun. Standards Mag.*, vol. 4, no. 1, pp. 34–41, Mar. 2020.

[67] M. A. Al-Shabi, "A comprehensive study of dissemination and data retrieval in secure VANET-cloud environment," in *Advances on Smart and Soft Computing*. Singapore: Springer, 2021, pp. 577–585.

[68] M. K. Priyan and G. U. Devi, "A survey on Internet of Vehicles: Applications, technologies, challenges and opportunities," *Int. J. Adv. Intell. Paradigms*, vol. 12, no. 1/2, p. 98, 2019.

[69] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 11, pp. 7015–7029, Nov. 2021.

[70] T. K. Priyambodo, D. Wijayanto, and M. S. Gitakarma, "Performance optimization of MANET networks through routing protocol analysis," *Computers*, vol. 10, no. 1, p. 2, Dec. 2020.

[71] M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," *Comput. Netw.*, vol. 79, pp. 166–187, Mar. 2015.

[72] W. Vandenberghe, I. Moerman, and P. Demeester, "Adoption of vehicular ad hoc networking protocols by networked robots," *Wireless Pers. Commun.*, vol. 64, no. 3, pp. 489–522, Jun. 2012.

[73] R. Al-Zaidi, J. C. Woods, M. Al-Khalidi, and H. Hu, "Building novel VHF-based wireless sensor networks for the Internet of marine things," *IEEE Sensors J.*, vol. 18, no. 5, pp. 2131–2144, Mar. 2018.

[74] A. Tufail, M. Fraser, A. Hammad, K. K. Hyung, and S.-W. Yoo, "An empirical study to analyze the feasibility of WiFi for VANETs," in *Proc. 12th Int. Conf. Comput. Supported Cooperat. Work Design*, Apr. 2008, pp. 553–558.

[75] M. Wellens, B. Westphal, and P. Mahonen, "Performance evaluation of IEEE 802.11-based WLANs in vehicular scenarios," in *Proc. IEEE 65th Veh. Technol. Conf. (VTC-Spring)*, Apr. 2007, pp. 1167–1171.

[76] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digit. Commun. Netw.*, vol. 3, no. 2, pp. 78–88, May 2017.

[77] N. Cen, J. Jagannath, S. Moretti, Z. Guan, and T. Melodia, "LANET: Visible-light ad hoc networks," *Ad Hoc Netw.*, vol. 84, pp. 107–123, Mar. 2019.

[78] C. Zeyu, "6G, LIFI and WiFi wireless systems: Challenges, development and prospects," in *Proc. 18th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Dec. 2021, pp. 322–325.

[79] Z. Liu, X. Han, Y. Liu, and Y. Wang, "D2D-based vehicular communication with delayed CSI feedback," *IEEE Access*, vol. 6, pp. 52857–52866, 2018.

[80] G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "LTE for vehicular networking: A survey," *IEEE Commun. Mag.*, vol. 51, no. 5, pp. 148–157, May 2013.

[81] S. Ucar, S. Ergen, and O. Ozkasap, "Multihop-cluster-based IEEE 802.11p and LTE hybrid architecture for VANET safety message dissemination," *IEEE Trans. Veh. Technol.*, vol. 65, no. 4, pp. 2621–2636, Apr. 2016.

[82] J. Choi, V. Va, N. G.-Prelcic, R. Daniels, C. R. Bhat, and R. W. Heath, Jr., "Millimeter-wave vehicular communication to support massive automotive sensing," *IEEE Commun. Mag.*, vol. 54, no. 12, pp. 160–167, Dec. 2016.

[83] V. Va, T. Shimizu, G. Bansal, and R. W. Heath, Jr., "Millimeter wave vehicular communications: A survey," *Found. Trends Netw.*, vol. 10, no. 1, pp. 1–113, 2016.

[84] S. A. A. Shah, E. Ahmed, M. Imran, and S. Zeadally, "5G for vehicular communications," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 111–117, Jan. 2018.

[85] 5GAA. *The Cost-Benefit Analysis on Cellular Vehicle to Everything (C-V2X) Technology and its Evolution to 5G-V2X*. Accessed: Jan. 21, 2022. [Online]. Available: http: https://www.5gaa.org/wpcontent/uploads/2017/12/Final-report-for-5GAA-on-cellular-V2Xsocio-economic-bene_ts-051217_FINAL.pdf

[86] A. Weissberger. *IEEE ComSoc Technology Blog*. 3GPP Release 16 Update. Accessed: Dec. 19, 2021. [Online]. Available: https://techblog.comsoc.org/2019/10/06/3gpp-release-16-update-5gphase-2-including-urllc-to-be-completed-in-june-2020/

[87] K. Wevers and M. Lu, "V2X communication for its-from IEEE 802.11 p towards 5G," *IEEE 5G Tech Focus*, vol. 1, no. 2, pp. 5–10, Jun. 2017.

[88] A. Filippi, K. Moerman, G. Daalderop, P. D. Alexander, F. Schober, and W. Piegl. (Apr. 2016). *Ready to Roll: Why 802.11 p Beats LTE and 5G for V2X*. NXP Semicond., Cohda Wireless, Siemens White Paper. Accessed: Dec. 28, 2021. [Online]. Available: https://assets.new.siemens.com/siemens/assets/public.1510309 207.ab5935c545ee430a94910921b-8ec75f3c17bab6c.its-g5-ready-to-roll-en.pdf

[89] M. Collotta, G. Pau, T. Talty, and O. K. Tonguz, "Bluetooth 5: A concrete step forward toward the IoT," *IEEE Commun. Mag.*, vol. 56, no. 7, pp. 125–131, Jul. 2018.

[90] J.-R. Lin, T. Talty, and O. Tonguz, "On the potential of Bluetooth low energy technology for vehicular applications," *IEEE Commun. Mag.*, vol. 53, no. 1, pp. 267–275, Jan. 2015.

[91] R. Frank, W. Bronzi, G. Castignani, and T. Engel, "Bluetooth low energy: An alternative technology for VANET applications," in *Proc. 11th Annu. Conf. Wireless On-Demand Netw. Syst. Services (WONS)*, Apr. 2014, pp. 104–107.

[92] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, ''Survey on vehicular ad hoc networks and its access technologies security vulnerabilities and countermeasures,'' 2019, *arXiv:1903.01541*.
[93] L. C. Hua, M. H. Anisi, L. Yee, and M. Alam, ''Social networking-based cooperation mechanisms in vehicular ad-hoc network—A survey,'' *Veh. Commun.*, vol. 10, pp. 57–73, Oct. 2017.
[94] F. Cunha, L. Villas, A. Boukerche, G. Maia, A. Viana, R. A. F. Mini, and A. A. F. Loureiro, ''Data communication in VANETs: Protocols, applications and challenges,'' *Ad Hoc Netw.*, vol. 44, pp. 90–103, Jul. 2016.
[95] N. Gupta, A. Prakash, and R. Tripathi, ''Medium access control protocols for safety applications in vehicular ad-hoc network: A classification and comprehensive survey,'' *Veh. Commun.*, vol. 2, no. 4, pp. 223–237, Oct. 2015.
[96] X. Zhao, S. Jing, F. Hui, R. Liu, and A. J. Khattak, ''DSRC-based rear-end collision warning system—An error-component safety distance model and field test,'' *Transp. Res. C, Emerg. Technol.*, vol. 107, pp. 92–104, Oct. 2019.
[97] R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas, and A. Alamoody, ''An overview on V2P communication system: Architecture and application,'' in *Proc. 3rd Int. Conf. Eng. Technol. Appl. (IICETA)*, Sep. 2020, pp. 174–178.
[98] A. M. R. Tolba, ''Trust-based distributed authentication method for collision attack avoidance in VANETs,'' *IEEE Access*, vol. 6, pp. 62747–62755, 2018.
[99] R. Shankar and A. V. Singh, ''Use of VANETs for human safety in road transportation,'' in *Proc. 4th Int. Conf. Rel., INFOCOM Technol. Optim. (ICRITO) (Trends Future Directions)*, Sep. 2015, pp. 1–6.
[100] Nidhi and D. K. Lobiyal, ''Performance evaluation of realistic VANET using traffic light scenario,'' 2012, *arXiv:1203.2195*.
[101] R. Florin and S. Olariu, ''A survey of vehicular communications for traffic signal optimization,'' *Veh. Commun.*, vol. 2, no. 2, pp. 70–79, Apr. 2015.
[102] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, ''A novel mechanism of detection of denial of service attack (DoS) in VANET using malicious and irrelevant packet detection algorithm (MIPDA),'' in *Proc. Int. Conf. Comput., Commun. Automat.*, May 2015, pp. 414–419.
[103] C. Hemalatha and T. V. Sarath, ''Analysis of clustering algorithm in VANET through co-simulation,'' in *Sustainable Communication Networks and Application*. Singapore: Springer, 2022, pp. 441–450.
[104] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, ''Cross-layer scheme for detecting large-scale colluding sybil attack in VANETs,'' in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2015, pp. 7298–7303.
[105] A. Gruebler, K. D. McDonald-Maier, and K. M. Ali Alheeti, ''An intrusion detection system against black hole attacks on the communication network of self-driving cars,'' in *Proc. 6th Int. Conf. Emerg. Secur. Technol. (EST)*, Sep. 2015, pp. 86–91.
[106] S. Sharma and B. Kaushik, ''Applications and challenges in Internet of Vehicles: A survey,'' in *Internet of Things and its Applications*. Singapore: Springer, 2022, pp. 55–65.
[107] R. Kumar and M. Dave, ''A review of various VANET data dissemination protocols,'' *Int. J. u- and e-Service*, vol. 5, no. 3, pp. 27–44, 2012.
[108] N. M. Mittal and P. Vashist, ''A detail survey on applications of vehicular ad-hoc networks (VANETs),'' *Int. J. Comput. Sci. Mobile Comput.*, vol. 3, no. 6, pp. 713–721, 2014.
[109] Y.-S. Chen, Y.-W. Lin, and S.-L. Lee, ''A mobicast routing protocol in vehicular ad-hoc networks,'' *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 20–35, Feb. 2010.
[110] R. Khatoun, P. Gut, R. Doulami, L. Khoukhi, and A. Serhrouchni, ''A reputation system for detection of black hole attack in vehicular networking,'' in *Proc. Int. Conf. Cyber Secur. Smart Cities, Ind. Control Syst. Commun. (SSIC)*, Aug. 2015, pp. 1–5.
[111] S. Reshma and C. Chetanaprakash, ''Advancement in infotainment system in automotive sector with vehicular cloud network and current state of art,'' *Int. J. Electr. Comput. Eng.*, vol. 10, no. 2, p. 2077, Apr. 2020.
[112] A. M. Said, M. Marot, A. W. Ibrahim, and H. Afifi, ''Modeling interactive real-time applications in VANETs with performance evaluation,'' *Comput. Netw.*, vol. 104, pp. 66–78, Jul. 2016.
[113] Y. Toor, P. Muhlethaler, A. Laouiti, and A. La Fortelle, ''Vehicle ad hoc networks: Applications and related technical issues,'' *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 2008.
[114] B. Alaya, R. Khan, T. Moulahi, and S. E. Khediri, ''Study on QoS management for video streaming in vehicular ad hoc network (VANET),'' *Wireless Pers. Commun.*, vol. 118, no. 4, pp. 1–33, 2021.
[115] M. M. Hamdi, L. Audah, S. A. Rashid, A. H. Mohammed, S. Alani, and A. S. Mustafa, ''A review of applications, characteristics and challenges in vehicular ad-hoc networks (VANETs),'' in *Proc. Int. Congr. Hum.-Comput. Interact., Optim. Robotic Appl.s (HORA)*, Jun. 202, pp. 1–7.
[116] S. Kumar and J. Singh, ''Internet of vehicles over VANETs: Smart and secure communication using IoT,'' *Scalable Comput., Pract. Exper.*, vol. 21, no. 3, pp. 425–440, Aug. 2020.
[117] M. A. Labiod, M. Gharbi, F.-X. Coudoux, P. Corlay, and N. Doghmane, ''Cross-layer scheme for low latency multiple description video streaming over vehicular ad-hoc NETworks (VANETs),'' *AEU Int. J. Electron. Commun.*, vol. 104, pp. 23–34, May 2019.
[118] S. Majumder, D. C. Mandava, J. Kim, and A. Y. Javaid, ''Multimedia transmission for V2X communication over legacy LTE—A network infrastructure—A performance evaluation,'' in *Proc. 11th IEEE Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf. (UEMCON)*, Oct. 2020, pp. 28–34.
[119] Z. Fantian, L. Chunxiao, Z. Anran, and H. Xuelong, ''Review of the key technologies and applications in Internet of Vehicle,'' in *Proc. 13th IEEE Int. Conf. Electron. Meas. Instrum. (ICEMI)*, Oct. 2017, pp. 228–232.
[120] F. Farouk, Y. Alkady, and R. Rizk, ''Efficient privacy-preserving scheme for location based services in VANET system,'' *IEEE Access*, vol. 8, pp. 60101–60116, 2020.
[121] N. E. Bezai, B. Medjdoub, A. Al-Habaibeh, M. L. Chalal, and F. Fadli, ''Future cities and autonomous vehicles: Analysis of the barriers to full adoption,'' *Energy Built Environ.*, vol. 2, no. 1, pp. 65–81, Jan. 2021.
[122] Z. Mahmood, ''Connected vehicles: A vital component of smart transportation in an intelligent city,'' in *Developing and Monitoring Smart Environments for Intelligent Cities*. Hershey, PA, USA: IGI Global, 2021, pp. 198–215.
[123] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, ''Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects,'' *IEEE Access*, vol. 4, pp. 5356–5373, 2016.
[124] J. Zhu, Y. Feng, and B. Liu, ''PASS: Parking-lot-assisted carpool over vehicular ad hoc networks,'' *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 1, Jan. 2013, Art. no. 491756.
[125] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, ''VANET security surveys,'' *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[126] H. T. Cheng, H. Shan, and W. Zhuang, ''Infotainment and road safety service support in vehicular networking: From a communication perspective,'' *Mech. Syst. Signal Process.*, vol. 25, no. 6, pp. 2020–2038, Aug. 2011.
[127] M. Contreras and E. Gamess, ''An algorithm based on VANET technology to count vehicles stopped at a traffic light,'' *Int. J. Intell. Transp. Syst. Res.*, vol. 18, no. 1, pp. 122–139, Jan. 2020.
[128] N. Bermad, S. Zemmoudj, and M. Omar, ''Context-aware negotiation, reputation and priority traffic light management protocols for VANET-based smart cities,'' *Telecommun. Syst.*, vol. 72, no. 1, pp. 131–153, Sep. 2019.
[129] F. Arena, G. Pau, and A. Severino, ''A review on IEEE 802.11 p for intelligent transportation systems,'' *J. Sensor Actuator Netw.*, vol. 9, no. 2, p. 22, 2020.
[130] F. D. Cunha, A. Boukerche, L. Villas, A. C. Viana, and A. F. Loureiro, ''Data communication in VANETs: A survey, challenges and applications,'' INRIA Saclay, Paris-Saclay Univ., Res. Rep. RR-8498, Mar. 2014.
[131] A. R. Abdellah and A. Koucheryavy, ''VANET traffic prediction using LSTM with deep neural network learning,'' in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Cham, Switzerland: Springer, 2014, pp. 281–294.
[132] R. A. Mallah, A. Quintero, and B. Farooq, ''Distributed classification of urban congestion using VANET,'' *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2435–2442, Sep. 2017.
[133] P. Kamal, R. S. Raw, N. Singh, S. Kumar, and A. Kumar, ''VANET based health monitoring through wireless body sensor network,'' in *Proc. 3rd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2016, pp. 2865–2871.
[134] P. Singh, R. S. Raw, and S. A. Khan, ''Development of novel framework for patient health monitoring system using VANET: An Indian perspective,'' *Int. J. Inf. Technol.*, vol. 13, no. 1, pp. 383–390, Feb. 2021.
[135] S. Uma and R. Eswari, ''Accident prevention and safety assistance using IoT and machine learning,'' *J. Reliable Intell. Environ.*, vol. 8, no. 2, pp. 1–25, 2021.

[136] Q. Abbas and A. Alsheddy, "Driver fatigue detection systems using multi-sensors, smartphone, and cloud-based computing platforms: A comparative analysis," *Sensors*, vol. 21, no. 1, p. 56, Dec. 2020.
[137] Y. Agarwal, K. Jain, and O. Karabasoglu, "Smart vehicle monitoring and assistance using cloud computing in vehicular ad hoc networks," *Int. J. Transp. Sci. Technol.*, vol. 7, no. 1, pp. 60–73, Mar. 2018.
[138] P. Singh, "Vehicle monitoring and surveillance through vehicular sensor network," in *Cloud-Based Big Data Analytics in Vehicular Ad-Hoc Networks*. Hershey, PA, USA: IGI Global, 2021, pp. 165–190.
[139] L. Pu, Z. Liu, Z. Meng, X. Yang, K. Zhu, and L. Zhang, "Implementing on-board diagnostic and GPS on VANET to safe the vehicle," in *Proc. Int. Conf. Connected Vehicles Expo (ICCVE)*, Oct. 2015, pp. 13–18.
[140] S. Khakpour, R. W. Pazzi, and K. El-Khatib, "Using clustering for target tracking in vehicular ad hoc networks," *Veh. Commun.*, vol. 9, pp. 83–96, Jul. 2017.
[141] S. Safavat, N. N. Sapavath, and D. B. Rawat, "Recent advances in mobile edge computing and content caching," *Digit. Commun. Netw.*, vol. 6, no. 2, pp. 189–194, May 2020.
[142] S. S. Alshamrani, N. Jha, and D. Prashar, "B5G ultrareliable low latency networks for efficient secure autonomous and smart Internet of vehicles," *Math. Problems Eng.*, vol. 2021, pp. 1–15, Sep. 2021.
[143] S. Singh, S. Negi, S. K. Verma, and N. Panwar, "Comparative study of existing data scheduling approaches and role of cloud in VANET environment," *Proc. Comput. Sci.*, vol. 125, no. 2, pp. 925–934, 2018.
[144] L. Zhang, D. Gao, W. Zhao, and H.-C. Chao, "A multilevel information fusion approach for road congestion detection in VANETs," *Math. Comput. Model.*, vol. 58, nos. 5–6, pp. 1206–1221, Sep. 2013.
[145] N. Monir, M. M. Toraya, A. Vladyko, A. Muthanna, M. A. Torad, F. E. A. El-Samie, and A. A. Ateya, "Seamless handover scheme for MEC/SDN-based vehicular networks," *J. Sensor Actuator Netw.*, vol. 11, no. 1, p. 9, Jan. 2022.
[146] N. Ganeshkumar and S. Kumar, "OBU (on-board unit) wireless devices in VANET(s) for effective communication—A review," in *Computational Methods and Data Engineering*. Singapore: Springer, 2021, pp. 191–202.
[147] M. A. Javed and J. Y. Khan, "A cooperative safety zone approach to enhance the performance of VANET applications," in *Proc. IEEE 77th Veh. Technol. Conf. (VTC Spring)*, Jun. 2013, pp. 1–5.
[148] A. Santamaria, M. Tropea, P. Fazio, and F. De Rango, "Managing emergency situations in VANET through heterogeneous technologies cooperation," *Sensors*, vol. 18, no. 5, p. 1461, May 2018.
[149] L. Liu, S. Lu, R. Zhong, B. Wu, Y. Yao, Q. Zhang, and W. Shi, "Computing systems for autonomous driving: State of the art and challenges," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6469–6486, Apr. 2021.
[150] F. Arena, G. Pau, and A. Severino, "V2X communications applied to safety of pedestrians and vehicles," *J. Sensor Actuator Netw.*, vol. 9, no. 1, p. 3, Dec. 2019.
[151] R. M. Namugenyi, "Advancing transportation in Uganda with automation advancing transportation in Uganda with automation, connectivity and intelligence," Ph.D. dissertation, College Eng., Des., Art Technol. (CEDAT), Dept. Elect. Comput. Eng., Makerere Univ., 2018.
[152] A. Theofilatos, G. Yannis, P. Kopelias, and F. Papadimitriou, "Impact of real-time traffic characteristics on crash occurrence: Preliminary results of the case of rare events," *Accident Anal. Prevention*, vol. 130, pp. 151–159, Sep. 2019.
[153] Y. L. Morgan, "Notes on DSRC & WAVE standards suite: Its architecture, design, and characteristics," *IEEE Commun. Surveys Tuts.*, vol. 12, no. 4, pp. 504–518, May 2010.
[154] I. Rasheed and F. Hu, "Intelligent super-fast vehicle-to-everything 5G communications with predictive switching between mmWave and THz links," *Veh. Commun.*, vol. 27, Jan. 2021, Art. no. 100303.
[155] L. Khamer, N. Labraoui, A. M. Gueroui, and A. A. A. Ari, "Enhancing video dissemination over urban VANETs using line of sight and QoE awareness mechanisms," *Ann. Telecommun.*, vol. 76, nos. 9–10, pp. 759–775, Oct. 2021.
[156] F. Pang, X. Bai, and M. Ran, "Research of applications of compressed sensing in VANET," in *Proc. IEEE 11th Int. Conf. Commun. Softw. Netw. (ICCSN)*, Jun. 2019, pp. 742–746.
[157] H. Faris and S. Yazid, "Development of communication technology on VANET with a combination of ad-hoc, cellular and GPS signals as a solution traffic problems," in *Proc. 7th Int. Conf. Inf. Commun. Technol. (ICoICT)*, Jul. 2019, pp. 1–9.
[158] S. M. Hussain, K. M. Yusof, R. Asuncion, S. A. Hussain, and A. Ahmad, "An integrated approach of 4G LTE and DSRC (IEEE 802.11p) for Internet of Vehicles (IoV) by using a novel cluster-based efficient radio interface selection algorithm to improve vehicular network (VN) performance," in *Sustainable Advanced Computing* (Lecture Notes in Electrical Engineering), vol. 840, S. Aurelia, S. S. Hiremath, K. Subramanian, and S. K. Biswas, Eds. Singapore: Springer, 2022, pp. 569–583, doi: 10.1007/978-981-16-9012-9_46.
[159] Z. Xu, X. Li, X. Zhao, and M. H. Zhang, "DSRC versus 4G-LTE for connected vehicle applications: A study on field experiments of vehicular communication performance," *J. Adv. Transp.*, pp. 1–12, Aug. 2017, doi: 10.1155/2017/2750452.
[160] F. Pervez, C. Yang, and L. Zhao, "Dynamic resource management to enhance video streaming experience in a C-V2X network," in *Proc. IEEE 92nd Veh. Technol. Conf. (VTC-Fall)*, Nov. 2020, pp. 1–5.
[161] J. Bhatia, R. Dave, H. Bhayani, S. Tanwar, and A. Nayyar, "SDN-based real-time urban traffic analysis in VANET environment," *Comput. Commun.*, vol. 149, pp. 162–175, Jan. 2020.
[162] A. Mejdoubi, H. Fouchal, O. Zytoune, and M. Ouadou, "A distributed predictive road traffic management system in urban VANETs," in *Proc. 15th Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Jun. 2019, pp. 37–42.
[163] Q. Chen, N. Cheng, X. Wang, and F. Liu, "Multi-metric opportunistic routing for VANETs in urban scenario," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery*, Oct. 2011, pp. 118–122.
[164] K. N. Qureshi, A. H. Abdullah, O. Kaiwartya, F. Ullah, S. Iqbal, and A. Altameem, "Weighted link quality and forward progress coupled with modified RTS/CTS for beaconless packet forwarding protocol (B-PFP) in VANETs," *Telecommun. Syst.*, vol. 75, no. 2, pp. 145–160, Oct. 2020.
[165] J. Qian, T. Jing, Y. Huo, Y. Li, W. Zhou, and Z. Li, "A next-hop selection scheme providing long path lifetime in VANETs," in *Proc. IEEE 26th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commun. (PIMRC)*, Aug. 2015, pp. 1929–1933.
[166] S. Das, "Analysis of next hop selection for geocasting in VANET," in *Proc. Int. Conf. Comput. Sci., Eng. Inf. Technol.* Berlin, Germany: Springer, 2011, pp. 326–335.
[167] O. Rehman and M. Ould-Khaoua, "A hybrid relay node selection scheme for message dissemination in VANETs," *Future Gener. Comput. Syst.*, vol. 93, pp. 1–17, Apr. 2019.
[168] J. Gozalvez, M. Sepulcre, and R. Bauza, "Impact of the radio channel modelling on the performance of VANET communication protocols," *Telecommun. Syst.*, vol. 50, no. 3, pp. 149–167, Jul. 2012.
[169] T. Abbas, K. Sjöberg, J. Karedal, and F. Tufvesson, "A measurement based shadow fading model for vehicle-to-vehicle network simulations," *Int. J. Antennas Propag.*, vol. 2015, pp. 1–12, 2015.
[170] K. Naseer, "Localization-based system challenges in vehicular ad hoc networks: Survey," *Smart Comput. Rev.*, vol. 4, no. 6, pp. 515–528, Dec. 2014.
[171] J. Chen, P. Rajib, and Y.-J. Choi, "An efficient neural network-based next-hop selection strategy for multi-hop VANETs," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 699–702.
[172] R. Purkait and S. Tripathi, "Fuzzy logic based multi-criteria intelligent forward routing in VANET," *Wireless Pers. Commun.*, vol. 111, no. 3, pp. 1871–1897, Apr. 2020.
[173] M. A. Saleem, Z. Shijie, M. U. Sarwar, T. Ahmad, A. Maqbool, C. S. Shivachi, and M. Tariq, "Deep learning-based dynamic stable cluster head selection in VANET," *J. Adv. Transp.*, vol. 2021, pp. 1–21, Jul. 2021.
[174] Y. Hao, T. Han, and Y. Cheng, "A cooperative message authentication protocol in VANETs," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 5562–5566.
[175] M. A. Al-Shareeda, M. Anbar, S. Manickam, and A. A. Yassin, "VPPCS: VANET-based privacy-preserving communication scheme," *IEEE Access*, vol. 8, pp. 150914–150928, 2020.
[176] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 770–790, Nov. 2018.
[177] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 5, pp. 2553–2571, May 2021.
[178] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cognit. Syst. Res.*, vol. 55, pp. 153–163, Jun. 2019.

[179] E. A. Feukeu and T. Zuva, "Dynamic broadcast storm mitigation approach for VANETs," *Future Gener. Comput. Syst.*, vol. 107, pp. 1097–1104, Jun. 2020.
[180] S. Glass, I. Mahgoub, and M. Rathod, "Leveraging MANET-based cooperative cache discovery techniques in VANETs: A survey and analysis," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2640–2661, May 2017.
[181] I. Achour, F. Alfayez, and A. Busson, "A robust and efficient adaptive data dissemination protocol based on smart relay selection in vehicular networks," *Wireless Netw.*, vol. 27, no. 7, pp. 4497–4511, Oct. 2021.
[182] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and End-to-End authentication," *IEEE Access*, vol. 6, pp. 46558–46567, 2018.
[183] G. D'Angelo, A. Castiglione, and F. Palmieri, "A cluster-based multidimensional approach for detecting attacks on connected vehicles," *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12518–12527, Aug. 2021.
[184] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, and M. S. Obaidat, "A systematic review on security issues in vehicular ad hoc network," *Secur. Privacy*, vol. 1, no. 5, p. e39, Sep. 2018.
[185] *Security Architecture for Systems Providing End-to-End Communications*, document ITU-T X.805, 2003. [Online]. Available: https://www.itu.int/rec/T-REC-X.805-200310-I/en
[186] B. Ali, M. A. Gregory, and S. Li, "Multi-access edge computing architecture, data security and privacy: A review," *IEEE Access*, vol. 9, pp. 18706–18721, 2021.
[187] S. A. Rashid, L. Audah, M. M. Hamdi, M. S. Abood, and S. Alani, "Reliable and efficient data dissemination scheme in VANET: A review," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 6, pp. 6423–6434, 2020.
[188] Y. Cao, H. Zhang, X. Zhou, and D. Yuan, "A scalable and cooperative MAC protocol for control channel access in VANETs," *IEEE Access*, vol. 5, pp. 9682–9690, 2017.
[189] R. S. Batth, M. Gupta, K. S. Mann, S. Verma, and A. Malhotra, "Comparative study of TDMA-based MAC protocols in VANET: A mirror review," in *Proc. Int. Conf. Innov. Comput. Commun.* Singapore: Springer, 2020, pp. 107–123.
[190] V. Nguyen, C. Pham, T. Oo, N. Tran, E.-N. Huh, and C. S. Hong, "MAC protocols with dynamic interval schemes for VANETs," *Veh. Commun.*, vol. 15, pp. 40–62, Jan. 2018.
[191] S. Chaudhary, R. Ramjee, M. Sivathanu, N. Kwatra, and S. Viswanatha, "Balancing efficiency and fairness in heterogeneous GPU clusters for deep learning," in *Proc. 15th Eur. Conf. Comput. Syst.*, Apr. 2020, pp. 1–16.
[192] K. Bok, J. Lim, S. Hong, and J. Yoo, "A multiple RSU collaborative scheduling scheme for data services in vehicular ad hoc networks," *Cluster Comput.*, vol. 20, no. 2, pp. 1167–1178, Jun. 2017.
[193] T. S. J. Darwish, K. A. Bakar, O. Kaiwartya, and J. Lloret, "TRADING: Traffic aware data offloading for big data enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6869–6879, Jul. 2020.
[194] H. Zhou, H. Wang, X. Li, and V. Leung, "A survey on mobile data offloading technologies," *IEEE Access*, vol. 6, pp. 5101–5111, 2018.
[195] A. Al-Hilo, M. Samir, C. Assi, S. Sharafeddine, and D. Ebrahimi, "A cooperative approach for content caching and delivery in UAV-assisted vehicular networks," *Veh. Commun.*, vol. 32, Dec. 2021, Art. no. 100391.
[196] C. Dobre, C. Fratila, and L. Iftode, "An approach to evaluating usability of VANET applications," in *Proc. 7th Int. Wireless Commun. Mobile Comput. Conf.*, Jul. 2011, pp. 801–807.
[197] H. Khelifi, S. Luo, B. Nour, and H. Moungla, "In-network caching in ICN-based vehicular networks: Effectiveness & performance evaluation," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2020, pp. 1–6.
[198] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of DSRC and cellular network technologies for V2X communications: A survey," *IEEE Trans. Veh. Technol.*, vol. 65, no. 12, pp. 9457–9470, Dec. 2016.
[199] E. Hossain, G. Chow, V. C. M. Leung, R. D. McLeod, J. Mišić, V. W. S. Wong, and O. Yang, "Vehicular telematics over heterogeneous wireless networks: A survey," *Comput. Commun.*, vol. 33, no. 7, pp. 775–793, May 2010.
[200] J. He, K. Yang, and H.-H. Chen, "6G cellular networks and connected autonomous vehicles," *IEEE Netw.*, vol. 35, no. 4, pp. 255–261, Jul. 2021, doi: 10.1109/MNET.011.2000541.
[201] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6G for vehicle-to-everything (V2X) communications: Enabling technologies, challenges, and opportunities," 2020, *arXiv:2012.07753*.
[202] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.
[203] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, Jan. 2019.
[204] J. Liu, J. Li, W. Li, and J. Wu, "Rethinking big data: A review on the data quality and usage issues," *ISPRS J. Photogramm. Remote Sens.*, vol. 115, pp. 134–142, May 2016.
[205] Z. Oughannou, I. Kandrouch, N. E. H. Chaoui, and H. Chaoui, "Proposal architecture based on fog computing allowing real-time analysis in smart cities," in *Proc. 7th Int. Conf. Optim. Appl. (ICOA)*, May 2021, pp. 1–7.
[206] Z. H. Ali, M. M. Badawy, and H. A. Ali, "A novel geographically distributed architecture based on fog technology for improving vehicular ad hoc network (VANET) performance," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 5, pp. 1539–1566, Sep. 2020.
[207] W. Zhao, "A survey on fog computing applications in Internet of vehicles," in *Proc. 2nd Int. Conf. Comput. Data Sci. (CDS)*, Jan. 2021, pp. 27–32.
[208] N. Cheng, F. Lyu, J. Chen, W. Xu, H. Zhou, S. Zhang, and X. S. Shen, "Big data driven vehicular networks," *IEEE Netw.*, vol. 32, no. 6, pp. 160–167, Nov./Dec. 2018.
[209] L. Nkenyereye, S. M. R. Islam, M. Bilal, M. Abdullah-Al-Wadud, A. Alamri, and A. Nayyar, "Secure crowd-sensing protocol for fog-based vehicular cloud," *Future Gener. Comput. Syst.*, vol. 120, pp. 61–75, Jul. 2021.
[210] I. Rasheed, "Enhanced privacy preserving and truth discovery method for 5G and beyond vehicle crowd sensing systems," *Veh. Commun.*, vol. 32, Dec. 2021, Art. no. 100395.
[211] J. Goswami and A. Saha, "Adoption of IoT in vehicular traffic control: An overview," in *Electronic Systems and Intelligent Computing* (Lecture Notes in Electrical Engineering), vol. 686, P. K. Mallick, P. Meher, A. Majumder, and S. K. Das, Eds. Singapore: Springer, 2020, doi: 10.1007/978-981-15-7031-5_8.
[212] S. M. Hatim, S. J. Elias, N. Awang, and M. Y. Darus, "VANETs and Internet of Things (IoT): A discussion," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 12, no. 1, p. 218, Oct. 2018.
[213] S. S. Shinde, R. M. Yadahalli, and R. Shabadkar, "Cloud and IoT-based vehicular ad hoc networks (VANET)," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, G. Singh, V. Jain, J. M. Chatterjee, and L. Gaur, Eds., 2021, pp. 67–82, doi: 10.1002/9781119761846.ch4.
[214] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, "Toward integrating vehicular clouds with IoT for smart city services," *IEEE Netw.*, vol. 33, no. 2, pp. 65–71, Mar. 2019.
[215] D. N. Vadhwani and S. Buch, "A novel approach for the ITS application to prevent accidents using wireless sensor network, IoT and VANET," in *Proc. IEEE Int. Conf. Electr., Comput. Commun. Technol. (ICECCT)*, Feb. 2019, pp. 1–7.
[216] A. Chehri, T. E. Ouahmani, and N. Hakem, "Mining and IoT-based vehicle ad-hoc NETwork: Industry opportunities and innovation," *Internet Things*, vol. 14, Jun. 2021, Art. no. 100117.
[217] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive Internet of Vehicles," *Comput. Commun.*, vol. 120, pp. 58–70, May 2018.
[218] K. F. Hasan, A. Overall, K. Ansari, G. Ramachandran, and R. Jurdak, "Security, privacy and trust: Cognitive Internet of Vehicles," 2021, *arXiv:2104.12878*.
[219] M. A. Rahim, M. A. Rahman, M. M. Rahman, A. T. Asyhari, M. Z. A. Bhuiyan, and D. Ramasamy, "Evolution of IoT-enabled connectivity and applications in automotive industry: A review," *Veh. Commun.*, vol. 27, Jan. 2021, Art. no. 100285.
[220] R. N. Channakeshava and M. Sundaram, "A study on energy-efficient communication in VANETs using cellular IoT," in *Intelligence Enabled Research*. Singapore: Springer, 2021, pp. 75–85.
[221] D. Cheng, C. Li, and N. Qiu, "The application prospects of NB-IoT in intelligent transportation," in *Proc. 4th Int. Conf. Adv. Electron. Mater., Comput. Softw. Eng. (AEMCSE)*, Mar. 2021, pp. 1176–1179.
[222] M. B. Hassan, S. Alsharif, H. Alhumyani, E. S. Ali, R. A. Mokhtar, and R. A. Saeed, "An enhanced cooperative communication scheme for physical uplink shared channel in NB-IoT," *Wireless Personal Commun.*, vol. 120, no. 3, pp. 2367–2386, 2021.

[223] M. N. Tahir and M. Katz, "Performance evaluation of IEEE 802.11p, LTE and 5G in connected vehicles for cooperative awareness," *Eng. Rep.*, vol. 4, no. 4, p. e12467, Apr. 2022.
[224] K. Liu, K. Xiao, P. Dai, V. C. S. Lee, S. Guo, and J. Cao, "Fog computing empowered data dissemination in software defined heterogeneous VANETs," *IEEE Trans. Mobile Comput.*, vol. 20, no. 11, pp. 3181–3193, Nov. 2021.
[225] P. Dai, F. Song, K. Liu, Y. Dai, P. Zhou, and S. Guo, "Edge intelligence for adaptive multimedia streaming in heterogeneous Internet of Vehicles," *IEEE Trans. Mobile Comput.*, early access, Aug. 19, 2021, doi: 10.1109/TMC.2021.3106147.
[226] A. Lakhan, M. Ahmad, M. Bilal, A. Jolfaei, and R. M. Mehmood, "Mobility aware blockchain enabled offloading and scheduling in vehicular fog cloud computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 4212–4223, Jul. 2021.
[227] X. Hou, Z. Ren, J. Wang, W. Cheng, Y. Ren, K.-C. Chen, and H. Zhang, "Reliable computation offloading for edge-computing-enabled software-defined IoV," *IEEE Internet Things J.*, vol. 7, no. 8, pp. 7097–7111, Aug. 2020.
[228] W. Duan, J. Gu, M. Wen, G. Zhang, Y. Ji, and S. Mumtaz, "Emerging technologies for 5G-IoV networks: Applications, trends and opportunities," *IEEE Netw.*, vol. 34, no. 5, pp. 283–289, Sep. 2020.
[229] L. Liang, H. Ye, G. Yu, and G. Y. Li, "Deep-learning-based wireless resource allocation with application to vehicular networks," *Proc. IEEE*, vol. 108, no. 2, pp. 341–356, Feb. 2020.
[230] S. Wang, F. Liu, and H. Xia, "Content-based vehicle selection and resource allocation for federated learning in IoV," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, Mar. 2021, pp. 1–7.
[231] Y. Zhang, M. Zhang, C. Fan, F. Li, and B. Li, "Computing resource allocation scheme of IOV using deep reinforcement learning in edge computing environment," *EURASIP J. Adv. Signal Process.*, vol. 2021, no. 1, pp. 1–19, Dec. 2021.
[232] T. P. Sharma and A. K. Sharma, "Heterogeneous-internet of vehicles (Het-IoV) in twenty-first century: A comprehensive study," in *Handbook of Computer Networks and Cyber Security*. Cham, Switzerland: Springer, 2020, pp. 555–584.
[233] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[234] R. Vilalta, S. Via, F. Mira, R. Casellas, R. Munoz, J. Alonso-Zarate, A. Kousaridas, and M. Dillinger, "Control and management of a connected car using SDN/NFV, fog computing and Yang data models," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, Jun. 2018, pp. 378–383.
[235] A. Moubayed and A. Shami, "Softwarization, virtualization, & machine learning for intelligent & effective V2X communications," 2020, *arXiv:2006.04595*.
[236] W. Huang, L. Ding, D. Meng, J.-N. Hwang, Y. Xu, and W. Zhang, "QoE-based resource allocation for heterogeneous multi-radio communication in software-defined vehicle networks," *IEEE Access*, vol. 6, pp. 3387–3399, 2018.
[237] A. Bhatia, K. Haribabu, K. Gupta, and A. Sahu, "Realization of flexible and scalable VANETs through SDN and virtualization," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Chiang Mai, Thailand, Jan. 2018, pp. 280–282.
[238] A. Moubayed, A. Refaey, and A. Shami, "Software-defined perimeter (SDP): State of the art secure solution for modern networks," *IEEE Network*, vol. 33, no. 5, pp. 226–233, Sep./Oct. 2019.
[239] E. L. R. Lucion and R. C. Nunes, "Software defined perimeter: Improvements in the security of single packet authorization and user authentication," in *Proc.44th Latin Amer. Comput. Conf. (CLEI)*, Oct. 2018, pp. 708–717.
[240] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2017, pp. 1–6.
[241] Y. Han, X. Tao, X. Zhang, and S. Jia, "Average service time analysis of a clustered VNF chaining scheme in NFV-based V2X networks," *IEEE Access*, vol. 6, pp. 73232–73244, 2018.
[242] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: Opportunities and solutions," *IEEE Netw.*, vol. 35, no. 2, pp. 152–159, Mar. 2021.
[243] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Trans. Commun.*, vol. 68, no. 8, pp. 4734–4746, Aug. 2020.
[244] Z. Yu, J. Hu, G. Min, Z. Zhao, W. Miao, and M. S. Hossain, "Mobility-aware proactive edge caching for connected vehicles using federated learning," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5341–5351, Aug. 2021.
[245] F. Ayaz, Z. Sheng, D. Tian, and Y. L. Guan, "A blockchain based federated learning for message dissemination in vehicular networks," 2021, *arXiv:2109.06667*.
[246] Y. Li, X. Tao, X. Zhang, J. Liu, and J. Xu, "Privacy-preserved federated learning for autonomous driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8423–8434, Jul. 2022.
[247] S. Samarakoon, M. Bennis, W. Saad, and M. Debbah, "Distributed federated learning for ultra-reliable low-latency vehicular communications," *IEEE Trans. Commun.*, vol. 68, no. 2, pp. 1146–1159, Feb. 2020.
[248] X. Kong, H. Gao, G. Shen, G. Duan, and S. K. Das, "FedVCP: A federated-learning-based cooperative positioning scheme for social Internet of Vehicles," *IEEE Trans. Computat. Social Syst.*, vol. 9, no. 1, pp. 197–206, Feb. 2022.
[249] M. V. S. da Silva, L. F. Bittencourt, and A. R. Rivera, "Towards federated learning in edge computing for real-time traffic estimation in smart cities," in *Proc. Anais do 4th Workshop de Computação Urbana*, 2020, pp. 166–177.
[250] H. Xiao, J. Zhao, Q. Pei, J. Feng, L. Liu, and W. Shi, "Vehicle selection and resource optimization for federated learning in vehicular edge computing," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 11073–11087, Aug. 2022.
[251] T. Zeng, O. Semiari, M. Chen, W. Saad, and M. Bennis, "Federated learning on the road: Autonomous controller design for connected and autonomous vehicles," 2021, *arXiv:2102.03401*.
[252] A. M. Elbir, B. Soner, S. Coleri, D. Gunduz, and M. Bennis, "Federated learning in vehicular networks," 2020, *arXiv:2006.01412*.
[253] J. Duan, S. E. Li, Y. Guan, Q. Sun, and B. Cheng, "Hierarchical reinforcement learning for self-driving decision-making without reliance on labelled driving data," *IET Intell. Transp. Syst.*, vol. 14, no. 5, pp. 297–305, 2020.
[254] K. Zhang, D. Si, W. Wang, J. Cao, and Y. Zhang, "Transfer learning for distributed intelligence in aerial edge networks," *IEEE Wireless Commun.*, vol. 28, no. 5, pp. 74–81, Oct. 2021.
[255] A. Hekmatmanesh, P. H. J. Nardelli, and H. Handroos, "Review of the state-of-the-art of brain-controlled vehicles," *IEEE Access*, vol. 9, pp. 110173–110193, 2021.
[256] Y. Lu, L. Bi, and H. Li, "Model predictive-based shared control for brain-controlled driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 21, no. 2, pp. 630–640, Feb. 2020.
[257] R. C. Moioli, P. H. J. Nardelli, M. T. Barros, W. Saad, A. Hekmatmanesh, P. Gória, A. S. de Sena, M. Dzaferagic, H. Siljak, W. van Leekwijck, D. Carrillo, and S. Latré, "Neurosciences and 6G: Lessons from and needs of communicative brains," 2020, *arXiv:2004.01834*.
[258] R. C. Moioli, P. H. J. Nardelli, M. T. Barros, W. Saad, A. Hekmatmanesh, P. E. G. Silva, A. S. de Sena, M. Dzaferagic, H. Siljak, W. Van Leekwijck, D. C. Melgarejo, and S. Latre, "Neurosciences and wireless networks: The potential of brain-type communications and their applications," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 3, pp. 1599–1621, Jun. 2021, doi: 10.1109/COMST.2021.3090778.
[259] Y. Yuan, Y. Zhao, B. Zong, and S. Parolari, "Potential key technologies for 6G mobile communications," *Sci. China Inf. Sci.*, vol. 63, no. 8, Aug. 2020, Art. no. 183301, doi: 10.1007/s11432-019-2789-y.
[260] Y. Lu and L. Bi, "Human behavior model-based predictive control of longitudinal brain-controlled driving," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 3, pp. 1361–1374, Mar. 2021.
[261] Z. Yan and X. Jian, "Research on brain-computer interface system for vehicle control based on motion imagination," in *Proc. 2nd Int. Conf. Big Data Artif. Intell.*, Apr. 2020, pp. 516–520.
[262] S. Liu, D. Zhang, M. Qiao, K. Wang, S. Zhao, Y. Yang, and T. Yan, "Mind controlled vehicle based on lidar SLAM navigation and SSVEP technology," in *Proc. 9th Int. Winter Conf. Brain-Comput. Interface (BCI)*, Feb. 2021, pp. 1–4.
[263] A. Hekmatmanesh, H. M. Azni, H. Wu, M. Afsharchi, M. Li, and H. Handroos, "Imaginary control of a mobile vehicle using deep learning algorithm: A brain computer interface study," *IEEE Access*, vol. 10, pp. 20043–20052, 2022, doi: 10.1109/ACCESS.2021.3128611.

[264] Y. Su, M. LiWang, L. Huang, X. Du, and N. Guizani, "Green communications for future vehicular networks: Data compression approaches, opportunities, and challenges," *IEEE Netw.*, vol. 34, no. 6, pp. 184–190, Sep. 2020.

[265] A. Ihsan, W. Chen, S. Zhang, and S. Xu, "Energy-efficient NOMA multicasting system for beyond 5G cellular V2X communications with imperfect CSI," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 8, pp. 10721–10735, Aug. 2022.

[266] M. Saimler and S. C. Ergen, "Power efficient communication interface selection in cellular vehicle to everything networks," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Marrakesh, Morocco, Apr. 2019, pp. 1–6.

[267] F. Jameel, W. U. Khan, N. Kumar, and R. Jantti, "Efficient power-splitting and resource allocation for cellular V2X communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3547–3556, Jun. 2021.

[268] Y. Dai, K. Zhang, S. Maharjan, and Y. Zhang, "Edge intelligence for energy-efficient computation offloading and resource allocation in 5G beyond," *IEEE Trans. Veh. Technol.*, vol. 69, no. 10, p. 12 175-12 186, Oct. 2020.

[269] X. Huang, R. Yu, D. Ye, L. Shu, and S. Xie, "Efficient workload allocation and user-centric utility maximization for task scheduling in collaborative vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 70, no. 4, pp. 3773–3787, Apr. 2021.

[270] H. Guo, J. Liu, J. Ren, and Y. Zhang, "Intelligent task offloading in vehicular edge computing networks," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 126–132, Aug. 2020.

[271] Y. Wang, "Research review of green vehicle routing optimization," in *Proc. IOP Conf. Earth Environ. Sci.*, vol. 632, Apr. 2021, Art. no. 032031.

[272] M. Ammous, S. Belakaria, S. Sorour, and A. Abdel-Rahim, "Optimal cloud-based routing with in-route charging of mobility-on-demand electric vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 7, pp. 2510–2522, Jul. 2019.

[273] X. Tang, S. Bi, and Y.-J. A. Zhang, "Distributed routing and charging scheduling optimization for Internet of electric vehicles," *IEEE Internet Things.*, vol. 6, no. 1, pp. 136–148, Feb. 2019.

[274] G. Ferro, M. Paolucci, and M. Robba, "Optimal charging and routing of electric vehicles with power constraints and time-of-use energy prices," *IEEE Trans. Veh. Technol.*, vol. 69, no. 12, pp. 14436–14447, Dec. 2020.

[275] J. Wang, K. Zhu, and E. Hossain, "Green Internet of Vehicles (IoV) in the 6G era: Toward sustainable vehicular communications and networking," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 1, pp. 391–423, Mar. 2022.

[276] S. K. Sharma, I. Woungang, A. Anpalagan, and S. Chatzinotas, "Toward tactile internet in beyond 5G era: Recent advances, current issues, and future directions," *IEEE Access*, vol. 8, pp. 56948–56991, 2020.

[277] E. C. Strinati, S. Barbarossa, J. L. Gonzalez-Jimenez, D. Ktenas, N. Cassiau, L. Maret, and C. Dehos, "6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 42–58, Sep. 2019.

[278] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1243–1274, 2nd Quart., 2019.

[279] S. Tanwar, S. Tyagi, I. Budhiraja, and N. Kumar, "Tactile internet for autonomous vehicles: Latency and reliability analysis," *IEEE Wireless Commun.*, vol. 26, no. 4, pp. 66–72, Aug. 2019.

[280] A. Ghansiyal, M. Mittal, and A. K. Kar, "Information management challenges in autonomous vehicles: A systematic literature review," *J. Cases Inf. Technol.*, vol. 23, no. 3, pp. 58–77, Jul. 2021.

[281] C. Chaccour, M. N. Soorki, W. Saad, M. Bennis, and P. Popovski, "Can terahertz provide high-rate reliable low latency communications for wireless VR?" 2020, *arXiv:2005.00536*.

[282] E. Steinbach, M. Strese, M. Eid, X. Liu, A. Bhardwaj, Q. Liu, M. Al-Ja'Afreh, T. Mahmoodi, R. Hassen, A. El Saddik, and O. Holland, "Haptic codecs for the tactile internet," *Proc. IEEE*, vol. 107, no. 2, pp. 447–470, Feb. 2019.

[283] N. Promwongsa, A. Ebrahimzadeh, D. Naboulsi, S. Kianpisheh, F. Belqasmi, R. Glitho, N. Crespi, and O. Alfandi, "A comprehensive survey of the tactile internet: State-of-the-art and research directions," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 472–523, 2021.

[284] D. van den Berg, R. Glans, D. De Koning, F. A. Kuipers, J. Lugtenburg, K. Polachan, and P. T. Venkata, "Challenges in haptic communications over the tactile internet," *IEEE Access*, vol. 5, pp. 23502–23518, 2017.

[285] I. F. Akyildiz, A. Kak, and S. Nie, "6G and beyond: The future of wireless communications systems," *IEEE Access*, vol. 8, pp. 133995–134030, 2020.

[286] P. Botsinis, D. Alanis, Z. Babar, H. V. Nguyen, D. Chandra, S. X. Ng, and L. Hanzo, "Quantum search algorithms for wireless communications," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1209–1242, Apr. 2019.

[287] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6G," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, Aug. 2020.

[288] M. Mosca, "Cybersecurity in an era with quantum computers: Will we be ready?" *IEEE Secur. Privacy*, vol. 16, no. 5, pp. 38–41, Sep./Oct. 2018.

[289] S. Ha, H. Lee, D. Won, and Y. Lee, "Quantum-resistant lattice-based authentication for V2X communication in C-ITS," in *Proc. 14th Int. Conf. Ubiquitous Inf. Manage. Commun. (IMCOM)*, Jan. 2020, pp. 1–8.

[290] N. Y. Ahn and D. H. Lee, "Physical layer security of autonomous driving: Secure vehicle-to-vehicle communication in a security cluster," *Ad-hoc Sensor Wireless Netw.*, vol. 45, nos. 3–4, pp. 293–336, 2019.

[291] S. Myeong and Y. Jung, "Administrative reforms in the fourth industrial revolution: The case of blockchain use," *Sustainability*, vol. 11, p. 3971, Jul. 2019.

[292] C. Linnhoff-Popien, "PlanQK—Quantum computing meets artificial intelligence," *Digitale Welt*, vol. 4, no. 2, pp. 28–35, Apr. 2020, doi: 10.1007/s42354-020-0257-9.

[293] B. Coll-Perales, J. Gozalvez, and M. Gruteser, "Sub-6 GHz assisted MAC for millimeter wave vehicular communications," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 125–131, Mar. 2019.

[294] P. Ji, H.-M. Tsai, C. Wang, and F. Liu, "Vehicular visible light communications with LED taillight and rolling shutter camera," in *Proc. IEEE 79th Veh. Technol. Conf. (VTC Spring)*, May 2014, pp. 1–6.

[295] H. Nguyen, X. Xiaoli, M. Noor-A-Rahim, Y. L. Guan, D. Pesch, H. Li, and A. Filippi, "Impact of big vehicle shadowing on vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6902–6915, Jul. 2020.

[296] M. Noor-A-Rahim, G. G. M. N. Ali, H. Nguyen, and Y. L. Guan, "Performance analysis of IEEE 802.11p safety message broadcast with and without relaying at road intersection," *IEEE Access*, vol. 6, pp. 23786–23799, 2018.

[297] A. Memedi and F. Dressler, "Vehicular visible light communications: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 161–181, Oct. 2021.

[298] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and challenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047–2077, 4th Quart., 2015.

[299] Z. Xiao and Y. Zeng, "An overview on integrated localization and communication towards 6G," 2020, *arXiv:2006.01535*.

[300] M. Z. Chowdhury, M. Shahjalal, S. Ahmed, and Y. M. Jang, "6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions," 2019, *arXiv:1909.11315*.

[301] X. Zhang, L. Chen, J. Qiu, and J. Abdoli, "On the waveform for 5G," *IEEE Commun. Mag.*, vol. 54, no. 11, pp. 74–80, Nov. 2016.

[302] S.-Y. Lien, S.-L. Shieh, Y. Huang, B. Su, Y.-L. Hsu, and H.-Y. Wei, "5G new radio: Waveform, frame structure, multiple access, and initial access," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 64–69, Jun. 2017.

[303] M. Renfors, X. Mestre, E. Kofidis, and F. Bader, *Orthogonal Waveforms and Filter Banks for Future Communication Systems*. New York, NY, USA: Academic, 2017.

[304] R. Hadani, S. Rakib, M. Tsatsanis, A. Monk, and R. Calderbank, "Orthogonal time frequency space modulation," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Mar. 2017, pp. 1–6.

[305] P. Raviteja, K. T. Phan, Y. Hong, and E. Viterbo, "Interference cancellation and iterative detection for orthogonal time frequency space modulation," *IEEE Trans. Wireless Commun.*, vol. 17, no. 10, pp. 6501–6515, Oct. 2018.

[306] G. D. Surabhi, R. M. Augustine, and A. Chockalingam, "On the diversity of uncoded OTFS modulation in doubly-dispersive channels," *IEEE Trans. Wireless Commun.*, vol. 18, no. 6, pp. 3049–3063, Jun. 2019.

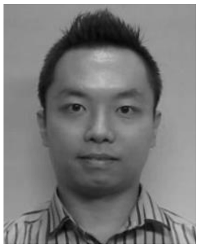
[307] S. Nayak and R. Patgiri, "6G communication: Envisioning the key issues and challenges," 2020, *arXiv:2004.04024*.

[308] S. Nayak, R. Patgiri, and T. D. Singh, "Big computing: Where are we heading?" *EAI Endorsed Trans. Scalable Inf. Syst.*, pp. 1–10, 2020, doi: 10.4108/eai.13-7-2018.163972.

[309] A. Kumari, S. Tanwar, S. Tyagi, and N. Kumar, "Verification and validation techniques for streaming big data analytics in Internet of Things environment," *IET Netw.*, vol. 8, no. 3, pp. 155–163, May 2018, doi: 10.1049/iet-net.2018.5187.

[310] R. Hasan and R. Hasan, "Towards a threat model and privacy analysis for V2P in 5G networks," in *Proc. IEEE 4th 5G World Forum (5GWF)*, Oct. 2021, pp. 383–387.
[311] M. Hamad and V. Prevelakis, "SAVTA: A hybrid vehicular threat model: Overview and case study," *Information*, vol. 11, no. 5, p. 273, May 2020.
[312] S. Myagmar, A. J. Lee, and W. Yurcik, "Threat modeling as a basis for security requirements," in *Proc. Symp. Requirements Eng. Inf. Secur.*, Aug. 2005, pp. 94–102.
[313] A. Shostack, *Threat Modeling: Designing for Security*. Indianapolis, IN, USA: Wiley, 2014.
[314] F. Ahmad, F. Kurugollu, A. Adnane, R. Hussain, and F. Hussain, "MARINE: Man-in-the-middle attack resistant trust model in connected vehicles," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3310–3322, Apr. 2020.
[315] M. Najafi, L. Khoukhi, and M. Lemercier, "A multidimensional trust model for vehicular ad-hoc networks," in *Proc. IEEE 46th Conf. Local Comput. Netw. (LCN)*, Oct. 2021, pp. 419–422.
[316] E. Qafzezi, K. Bylykbashi, P. Ampririt, M. Ikeda, K. Matsuo, and L. Barolli, "An intelligent approach for cloud-fog-edge computing SDN-VANETs based on fuzzy logic: Effect of different parameters on coordination and management of resources," *Sensors*, vol. 22, no. 3, p. 878, Jan. 2022.
[317] P. Arthurs, L. Gillam, P. Krause, N. Wang, K. Halder, and A. Mouzakitis, "A taxonomy and survey of edge cloud computing for intelligent transportation systems and connected vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 6206–6221, Jul. 2022.
[318] K. S. Kumar, A. R. Mani, S. Sundaresan, and T. A. Kumar, "Modeling of VANET for future generation transportation system through edge/fog/cloud computing powered by 6G," in *Cloud and IoT-Based Vehicular Ad Hoc Networks*, G. Singh, V. Jain, J. M. Chatterjee, and L. Gaur, Eds., 2021, pp. 105–124, doi: 10.1002/9781119761846.ch6.
[319] R. Bibi, Y. Saeed, A. Zeb, T. M. Ghazal, T. Rahman, R. A. Said, S. Abbas, M. Ahmad, and M. A. Khan, "Edge AI-based automated detection and classification of road anomalies in VANET using deep learning," *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–16, Sep. 2021.

**NEHAD HAMEED HUSSEIN** received the B.S. degree in computers and software engineering from the College of Engineering, Al-Mustansiriya University, Iraq, in 2007, and the M.S. degree in information engineering from the College of Information Engineering, Al-Nahrain University, Iraq, in 2011. He is currently pursuing the Ph.D. degree in electrical and communication engineering with the College of Engineering, Universiti Tenaga Nasional (UNITEN), Malaysia. He has participated in many research workshops and scientific conferences sponsored by IEEE, Springer, and IOP. His research interests include VANET, ad-hoc routing protocols, wireless communication optimization, network security, and signal processing.



**CHONG TAK YAW** received the bachelor's and master's degrees (Hons.) in electrical and electronics engineering and the Ph.D. degree in artificial neural network from the Universiti Tenaga Nasional (UNITEN), Malaysia, in 2008, 2012, and 2019, respectively. He is currently working as a Postdoctoral Researcher at the Institute of Sustainable Energy, UNITEN. His research interests include artificial neural networks and renewable energy.

**SIAW PAW KOH** received the bachelor's (Hons.), M.Sc., and Ph.D. degrees in electrical and electronic engineering from the Universiti Putra Malaysia, in 2000, 2002, and 2008, respectively. He is currently a Professor with the Institute of Sustainable Energy, Universiti Tenaga Nasional. His research interests include machine intelligence, automation technology, and renewable energy.

**SIEH KIONG TIONG** (Senior Member, IEEE) received the B.Eng. (Hons.), M.Sc., and Ph.D. degrees in electrical, electronic, and system engineering from the Nasional University of Malaysia (UKM), in 1997, 2000, and 2006, respectively. He is currently a Professor with the College of Engineering. He is also the Director of the Institute of Sustainable Energy (ISE), Universiti Tenaga Nasional. His research interests include renewable energy, artificial intelligence, data analytics, microcontroller systems, and communication systems. He is also a Professional Engineer registered with the Board of Engineers Malaysia (BEM).

**KOK HEN CHONG** received the Ph.D. degree from the Universiti Putra Malaysia, in 2008. He is currently an Associate Professor with the Universiti Tenaga Nasional, Malaysia. His consultancy, research, and development works involve control and automation system development, artificial intelligence techniques creation and innovation, electronic circuit design, and renewable energy research and applications.