Hindawi
Wireless Communications and Mobile Computing
Volume 2023, Article ID 9757532, 1 page
https://doi.org/10.1155/2023/9757532

Retraction

Retracted: A Taxonomy and Analysis on Internet of Vehicles: Architectures, Protocols, and Challenges

Wireless Communications and Mobile Computing

Received 12 December 2023; Accepted 12 December 2023; Published 13 December 2023

This article has been retracted by Hindawi, as publisher, following an investigation undertaken by the publisher [1]. This investigation has uncovered evidence of systematic manipulation of the publication and peer-review process. We cannot, therefore, vouch for the reliability or integrity of this article.

Please note that this notice is intended solely to alert readers that the peer-review process of this article has been compromised.

Wiley and Hindawi regret that the usual quality checks did not identify these issues before publication and have since put additional measures in place to safeguard research integrity.

We wish to credit our Research Integrity and Research Publishing teams and anonymous and named external researchers and research integrity experts for contributing to this investigation.

The corresponding author, as the representative of all authors, has been given the opportunity to register their agreement or disagreement to this retraction. We have kept a record of any response received.

References

[1] I. Seth, K. Guleria, S. N. Panda et al., "A Taxonomy and Analysis on Internet of Vehicles: Architectures, Protocols, and Challenges," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 9232784, 26 pages, 2022.

Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 9232784, 26 pages
https://doi.org/10.1155/2022/9232784

Review Article

A Taxonomy and Analysis on Internet of Vehicles: Architectures, Protocols, and Challenges

Ishita Seth,[1,2] Kalpna Guleria ,[1] Surya Narayan Panda ,[1] Divya Anand ,[3,4] Khalid Alsubhi ,[5] Hani Moaiteq Aljahdali ,[5] and Aman Singh [6]

[1]*Chitkara University Institute of Engineering and Technology, Chitkara University, Rajpura, 140401 Punjab, India*
[2]*Aptiv Components India Pvt. Ltd., India*
[3]*School of Computer Science and Engineering, Lovely Professional University, Punjab 144411, India*
[4]*Higher Polytechnic School, Universidad Europea del Atlántico, C/Isabel Torres 21, 39011 Santander, Spain*
[5]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 37848, Saudi Arabia*
[6]*Faculty of Engineering, Universidade Internacional do Cuanza, Estrada Nacional 250, Bairro Kaluapanda, Cuito-Bié, Angola*

Correspondence should be addressed to Kalpna Guleria; kalpna@chitkara.edu.in and Aman Singh; aman.singh@unic.co.ao

Received 11 March 2022; Accepted 22 April 2022; Published 30 May 2022

Academic Editor: Rashid A Saeed

The accelerated evolution in computing and transmission automation of the Internet of Vehicles (IoV) has led to enormous research standards that attract many researchers and industries. This century of the Internet of Things (IoT) is propulsive to the routine vehicular ad hoc networks (VANETs) in the IoV. It has emerged as one of the major driving forces for innovations in the intelligent vehicular industry. The World Health Organization (WHO) report confirms that approximately 1.35 million people die because of accidents on the road every year. This requires considerable attention to incorporate more and more safety measures into the automobile industry. Intelligent transportation systems can help bridge the gap between the traditional and the intelligent automotive industry by connecting vehicle to vehicle (V2V) and vehicle to infrastructure (V2I), hence adding much safety in vehicular communication. This paper provides a comprehensive review of the Internet of Vehicles (IoV) which discusses the architectures of IoV including layer types, functions of layers, application area, and communication type supported. Further, it also provides an in-depth insight into state-of-the-art Medium Access Control (MAC) protocols and routing protocols used in IoV communication. The routing protocol comparative summarization considers important parameters which include communication types broadcast, unicast, cluster, multicast, forwarding strategy, recovery strategy, availability of map, and the type of environment urban or highway. The summarization of various protocols highlights strengths, research gaps, and application areas. Finally, the paper addresses various research challenges along with potential future enhancements for the IoV communication.

1. Introduction

In today's era, the Internet of Things (IoT) has been playing a vital role to form the basis for technological developments in the vehicular ad hoc network, and it gears up much stimulus for various innovations on the Internet of Vehicles (IoV) [1, 2]. The IoV represents the interaction between the vehicle and the other Road Side Units (RSU). These units can be vehicles, roadside infrastructures, pedestrians, servers, etc. An Intelligent Transportation System (ITS) comprises a set of technologies and applications, and it is aimed at improving transportation safety and mobility while reducing accidental cases to the minimum possible. One of the most harmful effects of increased road traffic leads to an increase in road accidents. As per WHO statistics, millions of people lost their lives and get injuries due to road accidents; therefore, it is a global problem that needs to be addressed. In the current era, the Internet of Things (IoT) plays a vital role in communication; everything is getting connected to the Internet [3]. With the rapid increase in vehicular technology, the vehicular ad hoc network is slowly converting into the Internet of Vehicles (IoV). VANET turns every vehicle to join other vehicles by wireless communications as mentioned in Figure 1. However, it comes with the limitations of covering a small network that limits the flexibility and the number of connected vehicles. Further, few points like driver's behavior, challenging roads, and jams are the hindrances of VANET communication. Hence, it would be right to mention that in VANET; the involvement of objects is unstable and random. Therefore, the VANET was not enough to provide the services or the applications to its customers, and these reasons initiated the inception of IoV. The IoV majorly has two technologies that are vehicle intelligence and vehicle networking. Vehicle networking combines VANET (interconnection of vehicles) + vehicle telematics (connected vehicles) + Internet of devices.

Vehicle intelligence emphasizes the combination of various applications which support artificial intelligence, deep learning, and swarm computing, etc. to improve the safety of the driver and to achieve enhanced safety in vehicular technology [4, 5]. Many Original Equipment Manufacturers (OEMs) are now working towards vehicle intelligence, including Toyota, BMW, GWM, Volvo, and Ford [6–8]. Furthermore, various IT companies like Apple, Google, and Huawei are working to contribute to intelligent-vehicle systems [9–11]. Hence, the IoV is a combination of vehicles, an intelligent environment, humans, smart things, and a vast network that provides services in large cities. IoV is considered an integrated system with features like high conformity, controllability, validity, and numerous vehicles, networks, users, and smart devices [12]. IoV is the deep integration of the user-vehicle-device-environment that extends to provide an efficient service level to the users as per their expectations and satisfaction [13]. It is also called VANET, which is like a subset of IoV. IoV has telematics, defined as a technology based on wireless networks, that helps send, receive, and store the data, including speed, times, faults, consumption, and more. Also, from the past years, an enormous number of users have been included in the evolution of IoT, Big Data, and cloud computing. IT companies have published many applications or services, but VANET lacks the capacity to process complete information; hence, it can be used on small-scale applications, which generally reduces the number of users. Therefore, the traditional VANET, telematics, and other connected vehicle networks need something on a large scale. Hence, the Internet of Vehicles (IoV) came into existence.

It is required to highlight why it is impossible to achieve the same with the usage and application-level support of IoT [14]. The reason behind this is that some aspects of IoV are distinctive from IoT. IoT majorly targets the objects and provides the data for connecting things, whereas the Internet targets the user and serves the utility for the users. IoT is a platform for connecting the things that we use daily and embedded with sensors, software, and electronics to the Internet and enabling them to gather and exchange information. Information can be anything or everything; however, IoV majorly concentrates on integrating users and vehicles wherein users and vehicles can interchangeably act as an intelligence of each other. The network models in IoV are also quite different from the IoT and Internet.

Most of the researchers are working on V2V and V2I communication as it provides safety-related information well in advance to the driver of the vehicle, which helps save lives and time. Furthermore, Intelligent Transportation System (ITS) focuses primarily on safety and latency-sensitive services like collision detection, route navigation, traffic management, or emergency alert-related information that are supported via V2V and V2I communication. The Intelligent Transportation System (ITS) is an application that provides services related to transportation and traffic management to make lives better and provide safety to drivers and passengers. The main reason for the development of ITS was various road accidents, pollution, and traffic congestion, mainly in the metro cities. Road accidents are a significant concern for the driver and the passengers. ITS is the backbone for the development of next-generation technologies. It incorporates various fields like management of transportation, control of the traffic, and different policies. Wider areas of the ITS are information management, incident and emergency systems, Electronic Toll Collection, traffic management, etc. Recently, India has successfully implemented automatic toll gates [10, 15], equipped with sensors that sense the vehicle, scan the QR code associated with the vehicle, and automatically collect the toll cost.

In taxonomy of IoV communication, essentially, IoV has the foundation in five types of network communication [16], as illustrated in Figure 2. Vehicle-to-Vehicle (V2V) communication supports the exchange of information with outside vehicles. With the help of V2V, each vehicle acts as a node and tries to connect to the other moving vehicles. The network created by V2V is of a wide range, as shown in Figure 3. The information like the crash event on the route can quickly be passed from one vehicle to another vehicle with the help of V2V communication. The communication shall be quick enough without much delay so that the other vehicle receives the information without any delay [17–19].

Vehicle-to-Personal devices (V2P) bring attention to applications like Carplay and android auto support in vehicles. In this era, when the hands-free profile is in use, with the help of Android and iOS platform, it is easy to connect personal devices to the infotainment unit of the vehicle and communicate with the personal devices. The phone application can be replicated over the infotainment display, and the usage of applications like call, music, navigation, SIRI, and Google assistant can be made available for the driver to use without taking phones in the hands [20–22]. Vehicle-to-Server (V2S) supports the additional information accessible from the APIs with the help of the Internet. Now, it is possible to update the vehicle software by Over the Air (OTA) communication using V2S-based network communication. This is essential for the communication from the servers and any information update [20, 22, 23]. Vehicle-to-Infrastructure (V2I) supports the communication with the building or infrastructure of the city. In this type of application, drivers can easily be aware of the parking space availability in the malls and other scenarios like the availability of tables for food in some malls [17, 24, 25]. Vehicle-to-Roadside unit (V2R) is used to communicate with roadside units like traffic signals or warning signs for the road walk.

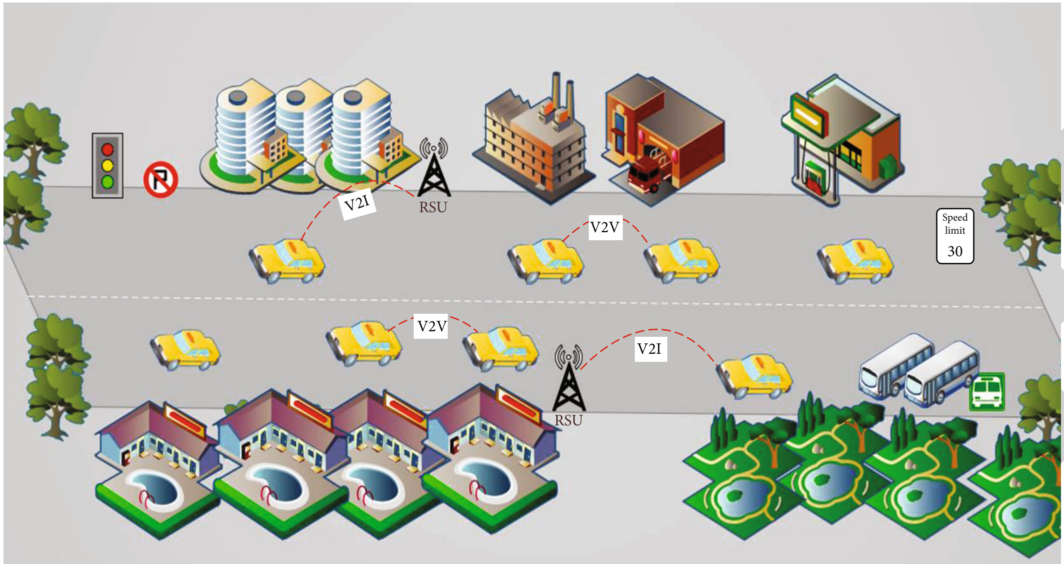

Figure 1: Types of communications in vehicular ad hoc networks (VANETs).

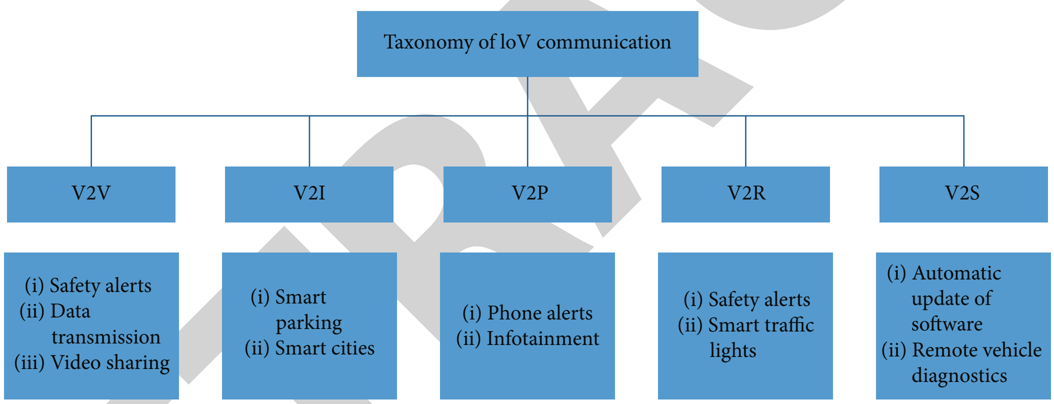

Figure 2: A taxonomy based on the of Internet of Vehicles (IoV) communication.

Also, while communicating between the vehicles in a dense network packet loss is the problem; considering the use of RSU, the communication between the vehicles can be maintained effectively [7, 20].

The main contribution of this review paper is as mentioned below:

The paper offers a deep dive into the various architectures of IoV proposed by the researchers in the past and a brief overview of the layered architecture. After a detailed analysis of the architecture, a comparison has been provided based on the number of layers, functions of layers, application area, and communication type supported.

The most relevant MAC protocol IEEE 802.11 has been discussed, and the comparison of the IEEE 802.11 series is provided concerning the different parameters of the communication at the MAC layer.

This paper spotlights the various routing protocols used in IoV for the communication between vehicle to vehicle and vehicle to infrastructure with a detailed description. Further, based on the communication types as broadcast, unicast, cluster, and multicast, the comparison has been provided. Also, the parameters for the communication like forwarding strategy, recovery strategy, and the environment for the protocols have been elaborated.

This paper provides the performance analysis of most popular state-of-the-art IoV routing protocols while considering packet delivery ratio (PDR), end-to-end (E2E) delay, and packet drop ratio.

Finally, various challenges concerning IoV communication have been discussed, and detailed summarization about state-of-the-art protocols has been discussed which elaborates their applicability and future enhancement needed.

The remaining paper is organized as follows: Section 2 discusses the previous reviews carried out in the domain of IoV. Section 3 elaborates various architectures proposed for IoV communication. Section 4 describes the various state-of-the-art routing protocols for vehicular communication. Section 5 discusses on the experimental analysis for the major routing protocols in the IoV. Section 6 summarizes the comparison of the various architectures, MAC and

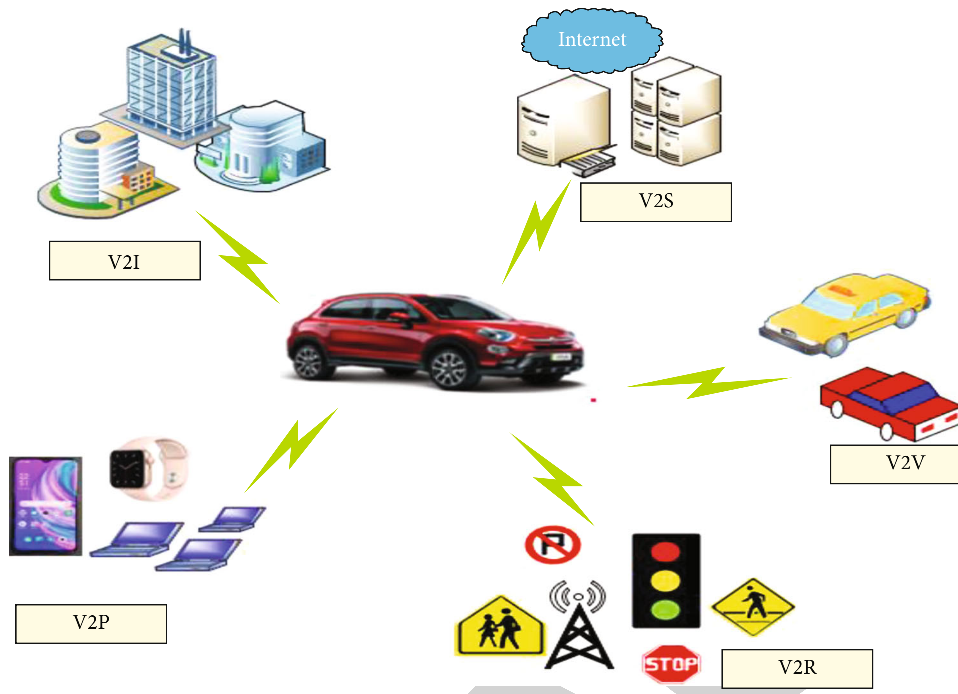

Figure 3: Types of communication supported in Internet of Vehicles (IoV).

routing protocols. Section 7 elaborates the characteristics, applications, and challenges in the IoV. Section 8 finally concludes the paper.

2. Related Work

This section elaborates on various existing works in the field of IoV. In the past years, researchers have accomplished various studies to explore the domain of IoV, standards, and applications.

In [15], the authors have provided a review on the IoV wherein the usage of the IoV in ITS has also been explained. The authors have elaborated on varied areas of ITS, mainly Incident and Emergency Management Systems, Information Management (IM) systems, and Transit Management Systems (TMS). The paper elaborates on multiple applications that support the ITS, such as Electronic Toll Collection (ETC), Traffic Management Systems (TMS), Transit Signal Priority (TSP), Vehicle Data Collection (VDC), and Highway Data Collection (HDC). Further, communication protocols for data-driven ITS environment need to be explored.

In [6], the authors have provided a review on IoV, which provides the details of state-of-the-art connectivity in the IoV and challenges. The authors have also emphasized that to enable the connectivity for wireless communication, there should be many radio interfaces that need to be implemented and may occur at a considerable cost. However, in time-bounded applications, the V2S connectivity may not be much efficient since it increases the delay.

In [26], the authors have discussed the taxonomy of routing protocols along with advantages and disadvantages. The analysis and architectural components of the VANETs have been discussed. Routing protocols based on the topology, clustering, hybrid, geographic, and data fusion have been elaborated. Application-specific protocols for IoV communication are still an open area to be explored.

In [27], the authors provided a review on the VANET and summarization of the applications for the VANET. The authors elaborated on comfort-related applications and safety-related applications. Further, the safety-related applications are subdivided into public safety, vehicle diagnostics, and information from another vehicle. The authors also have presented the differentiation between different simulations tools used in the VANET communication. However, the protocol level information at each layer of the architecture is still an area to be explored.

In [28], the authors discussed VANET routing protocols, especially those protocols that outperform in the city scenarios, considering the parameters, which included the obstacles, vehicle density, and the number of nodes. The comparison of position, topology, and cluster-based protocols has been presented along with their advantages and disadvantages. Further, emphasis is required to explore the information about the protocols based on the highway scenarios.

In [29], the authors have elaborated the protocols in the position-based category. The authors proposed categorization based on transmission strategy: unicast, geo-cast, and broadcast. Secondly, the information needed to perform routing is divided into four main categories: topology, position, map, and path based. The paper also provides differentiation based on the delay-tolerant and applicability in dimensions like 1-D, 2-D, and sensitive and delay 3-D. However, nondelay tolerant (NDT) is still an open area to be explored.

In [25], the authors have reviewed routing protocols based on the position, topology, and cluster-based. The paper also provides a comparative study and analysis of various routing protocols based on the performance metrics, speed, simulation tools, protocols in comparison, topology size, etc., whereas the hybrid VANET protocols can be explored based on the different ITS applications.

In [30], the authors have reviewed the routing protocols in IoV and their applications. Categorization of the routing protocols has been discussed into unicast, multicast, and broadcast. The authors have also discussed the applications of IoV based on the safety, commercial, convenience, and productivity level. Further, the best suited routing protocols based on specific application are yet to be explored.

In [31], the authors outlined the geographical routing protocols and paradigms used in the IoV routing. The paper emphasized the optimization techniques that included computational intelligence, cloud computing, and fog computing with the multioptimization-based routing protocols. The discussion is based on the three layers of IoV architecture with three different domains: marine, aerial, and terrestrial. Further, five-layer and seven-layer IoV architectures have not been taken into consideration.

The literature review as mentioned in Table 1 reveals that although there exist studies about IoV communication and routing and IoV architecture, however, there is still a gap to explore recent developments and an in-depth review of various IoV communication architecture, protocol, and application challenges. The paper provides a detailed discussion on the comparison of various state-of-the-art communication architectures of IoV, routing protocols, and MAC protocols. Further, it also addresses the research challenges in this domain while highlighting state-of-the-art in these fields of IoV.

3. Layered Architectures of IoV

The main inclinations of the IoV environment are to solve the problem of the connection between multiple devices in multiple fields (traffic management, security and entertainment, and information). However, due to privacy, usability, and accessibility issues, the interaction of these applications has limitations, so they usually act as independent entities [32, 33]. To reduce such problems, several attempts have been made by various researchers who focused on the development of cross interoperability platforms, elements, and devices from different vehicles that can collaborate in the environment of IoV [34–36].

In [34], the author proposed a three-tier architecture (client, connection, and cloud) of IoV. The client level consists of the sensors present inside and outside the vehicles that are responsible for gathering the information from the parameters like oil pressure and proximity, the vehicle speed, position of the destination vehicle, pressure of the tire, pollution level, crash detection, front obstacles, side obstacles, etc. Few parameters include the information related to vehicle incidents and driving behavior as well. The connection layer helps organize the routes for the data packets, and the cloud layer provides the computation power and retrieves the information from the network. To provide the foundation of the communication models between vehicle to vehicle, vehicle to sensors, vehicle to pedestrians, and vehicle to infrastructure, the connection layer provides interoperability with all networks available. It provides the computing power needed to meet all vehicle requirement needs (such as a shared communication spectrum, a repository for the data, the revival of the information, and analysis).

In [35], the authors suggested a four-layer architecture of IoV. The bottom layer uses the communication channel with the help of the 802.11p protocol, and it also includes the vehicle communication software used for V2V communication. The next layer is called an infrastructure layer, and it helps define the technology that enables the communication between everyone. The third layer is to review and implement all the appropriate controls and strategies for the information flow in the network. The top layer is the cloud, which specifies the type of cloud (public, private, or business) according to a specific configuration file and the ability to receive services (voice, business video, and data) when needed.

In [36], the authors proposed a three-tier architecture (vehicle, location, and cloud) of IoV. The vehicle layer controls all internal sensors of the vehicle and handles receiving information such as environmental parameters and physiological parameters that includes stress, heart rate, and emotions from the driver using short-range wireless technology. This architecture allows information to be exchanged with nearby vehicles as well as distant vehicles. Road Side Unit (RSU) is used to provide multihop communication. The cloud layer holds all the services that help to gather and access the historical traffic information. In addition to this, the layer can also help achieve load balancing across several interconnected cloud systems.

In [20], the authors described an architecture based on the five layers. It includes perception, coordination, artificial intelligence (AI), application, and business layers. The sensing layer contains the various kinds of sensors and actuators built in the vehicle, which gathers all the information from the different system elements. The coordination layer of vehicles, transportation environments, and connected devices (smartphones, tablets, headsets, and smartwatches) use universal coordination modules for network communication. It certifies the communication of information considering all the aspects of security for processing in the infrastructure based on the cloud, store, process, and analyze information. Other levels to make informed decisions for traffic safety, multimedia and infotainment systems, intelligent services, and the best applications for rigorous analysis of received information. The business layer is responsible for statistical analysis to generate the business strategies via diagrams, flowcharts, and comparison tables (using data, budget), which can be used to develop business models.

In [18], the authors proposed architecture for V2V communication. It has three layers. The first layer acts as the network area in which all the devices are connected directly or with the help of gateways that are further based on the wired or wireless communication. The middle layer supports the connectivity of the IP. Lastly, the top layer has all the applications which are IoV suitable for communication (smart homes and smart cities, etc.).

In [37], the authors proposed a heterogeneous architecture based on V2I data forwarding. The proposed

Table 1: State-of- the-art in IoV review and research gaps.

Ref. no	Year	Focus area	Research gaps
[15]	2011	IoV and ITS intelligent transportation system	Communication protocols for data-driven ITS environment need to be explored further
[6]	2014	IoV state-of-the-art connectivity and challenges	Application-specific protocols need to be emphasized
[26]	2014	VANET and its applications	Protocol at each level of the architecture is missing
[27]	2014	VANET architecture and protocols with pros and cons	Application-specific protocols for IoV communication need to be emphasized
[28]	2015	Routing in VANET and its simulations	Nondelay tolerant protocols are not taken into account
[29]	2019	VANET and routing in city scenarios	Highway scenarios need to be considered
[25]	2018	VANET transmission strategies are based on routing and its applications	Application-specific protocols need to be explored
[30]	2019	VANET routing protocols and the challenges in communication	Hybrid protocols for VANET are an open area to be explored
[31]	2020	Routing protocols of VANET and the optimization techniques	IoV protocols mapping on five-layer and seven-layer IoV architectures need to be explored

architecture works better compared to the IoV architectures based on the 4G, IEEE802.11p (WAVE), and IEEE802.11a/h (long-range Wi-Fi) architectures. The proposed architecture is based on the three-layer architecture. The bottom layer is the client layer. This layer handles the communication between the intervehicle and intravehicle. The middle layer is based on the connections and deals with the interconnection of the different networks within the automotive environment. The topmost layer is the cloud layer, which is answerable for handling all the applications and the services of IoV. Interaction with the other vehicles and the network entities are being managed by the cloud layer. The authors compared the results of the heterogeneous architecture of IoV with the conventional architecture and found the mentioned architecture outperforms on the parameters of high throughput and low latency.

In [32], the authors described the three-tier architecture for the IoV for secure communication. The division of the layers is tier 3, which contains all the vehicles on the road and equipped with the OBUs. The vehicles act as actuators and sensors for sensing the information from other vehicles or from the RSUs. Tier 3 is having V2V communication. Tier 2 is equipped with the Road Side Units (RSUs) and helps to facilitate the communication between the vehicles and with the other network devices. V2I communication mode is present in tier 2. Tier 1 consists of the cloud networks and the servers. The component central authority is also an important part of tier 1. It is responsible for the vehicle level characteristics which are present locally and globally. The central authority needs to check on the access information for verification of the vehicles. The major role of the cloud in the architecture is to share the information and the verification of the vehicle.

In [38], the authors elaborated an architecture for IoV-based Edge network for the optimal route selection with 5G technology in use. The authors proposed the multimodal architecture for IoV and took into consideration the data process for the smart cities that need the smart infrastructure to handle the huge amount of the data. In 5G communication, Cyber-Physical and Social Networks (CPSN), it is required to have a data-oriented architecture in place.

In [39], the authors have applied AI with Mobile edge computing (MEC) and analyzed the architecture based on both. Due to the increase of IoV and vehicle intelligence integration, vehicles are revamping into intelligent vehicles. However, due to the less battery capacity and computational power, it is challenging to handle the in-depth tasks within the vehicles. At first, the authors compared the traditional architecture with the 5G network coming up in place. Then, the authors described the advantage of using Mobile edge computing and AI in the IoV architecture. The most challenging part of IoV systems is the flawless assimilation of all the components that include the roadside infrastructure, personal devices, sensors, actuators, users, and vehicles to provide comfort and the safety levels to the user. In this case, the functionality needs to be enclosed into layers to provide the layer-based architecture of IoV systems. The main requirement is to design the number of layers required and the effectiveness of each layer that includes the network aspects and the communication mechanics.

In [40], upon designing the layered architecture, there were several issues that have been analyzed and need to be considered. These issues include the following: (a) to connect the several devices to diverse networks, (b) to adapt the latest technologies, and (c) to combine the Internet with service-oriented architecture and interface based on plug-and-play [24, 41].

3.1. Layered IoV Architecture. Although there are various layered architectures of IoV proposed by researchers, the most appropriate which supports all types of communication in IoV is discussed as follows: The layered IoV communication model architecture is described in Figure 4; there are seven layers that allow the translucent interrelationship of all the components in the network and data broadcasting in the IoV environment. The IoV model is founded on a user and the vehicle interface to command the communication between the user and the vehicle, layers to manage the

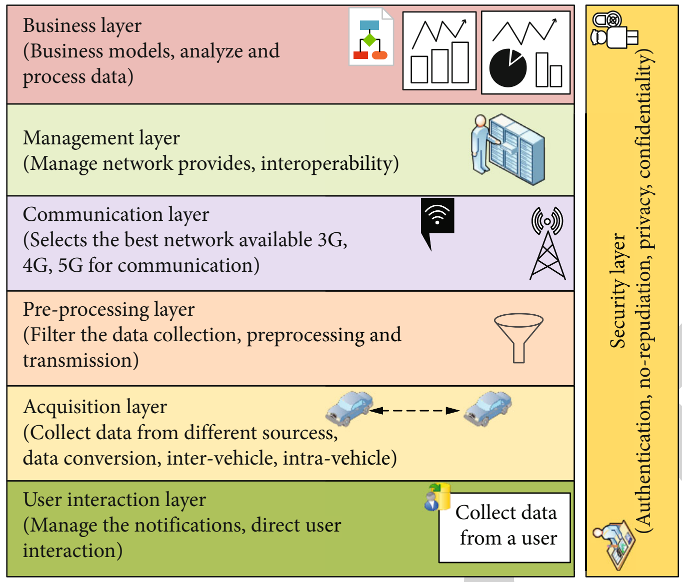

Figure 4: The seven-layer architecture of Internet of Vehicles (IoV) communication.

security, transaction authorization, and its accounting interface to communicate with other networks to deliver the information which is collected. For example, if a driver or passenger enables the Wi-Fi from the Infotainment display and tries to select the available Wi-Fi network, so based on the best service provider at that moment after consideration of the requirements needed for the communication, the profit of the vehicle, network connection and its quality, the cost of the transaction, etc. are selected.

In user interaction layer, there are mainly two types of communication systems in the vehicles, namely, information systems and control systems. The information system provides the required information such as information based on the route, traffic jam conditions, space availability for the parking, warnings, and notifications based on the occurrence of events. Also, it provides information regarding the driving environment, if the vehicle or the driver is at risk. There are several companies that are focusing on the design and development of solutions for IoV. As an example, there are several leading car manufacturers, including Google that developed Open Automotive. To realize the concept of connected cars (OAA, 2016, 21), an alliance is developed to provide the common Android platform. Apple has developed Carplay to enable iPhone services in cars (Apple, 2014, 21). To design the user interface is a challenging task to keep all the factors into consideration; like, it shall not divert the driver's mind and shall be satisfying the user's requirements while driving the vehicle [24, 41].

Further, there are applications such as adaptive cruise control, which controls the vehicle's speed automatically and helps to maintain speed, lane-keeping, and collision avoidance which helps to prevent drivers from the accidents and warn in case the accident is about to happen. It helps the driver to drive safely while meeting the user's needs. In data acquisition layer, this layer targets to gather the data which are related to the infotainment, safety-related information, the traffic information or from the areas selected by the interest of the driver that further includes global positioning system also known as GPS, body control module, road signals, and intervehicle communication. The data acquisition layer is basically for data, control, and management. This divides the streets into groups of neighboring clusters, and with help of cluster heads, the transmission of the data packets takes place further [24, 41]. It supports two types of data transmission, which include intravehicular interactions and intervehicular interactions. In the intravehicular interactions, the technologies like Bluetooth, Wi-Fi, and ZigBee were used, whereas intervehicular communication V2V, V2I, V2R, V2S, and V2P transmissions utilize the technology support for IEEE 802.11p for physical layer and MAC layers.

In data filtering and preprocessing layer, devices can bring out numerous data. However, the relevant data is needed by the system to process it. Hence, the collection of the data, filtering the data, and then circulating into the network is an important process in the IoV model. This layer helps to collect and then filter the data. To avoid traffic in the network, it is necessary that the right data is circulated on the network. In today's era, there are ample techniques present for data mining that are used to take out the relevant data efficiently and accurately process it [24, 41]. In the communication layer, there are many wireless technologies available for creating a heterogeneous communication network. Every network has its own features; hence, it is essential that they need to be combined in such a way that the connectivity shall not impact. The environment should provide the smooth connectivity of the services based on the different parameters like the relevance of information, security, privacy, and congestion in the network available. The major challenge is to select the appropriate network by accepting the required information. IoV takes many conditions into account when it needs to select the network which is used for the transmission so that the QoS for the applications remains at a higher level [24, 41].

In the control and management layer, the communication and management layers are liable for organizing the multiple network service providers present in the IoV environment. The approaches like management of traffic, engineering, inspection, and functional are being applied to receive the information in a manageable format. This layer helps in managing the network providers by taking interoperability requirements into consideration [24, 41]. In the business layer, it is also known as the processing layer. It is liable for a large amount of information by using the several available infrastructures of cloud computing that are present either locally or remotely. The basic function that is performed by this layer is to process and analyze the information received from other lower layers. The decision-making is based on statistical data analysis and strategizes on the business models as per the use of data in the application and the usage of tools like flowcharts and graphs. The obtained results can be used by many agencies, especially in the government centers, in the development of the infrastructure and the vehicle-to-business (V2B) to manage or improve road traffic [24, 41].

In the security layer, security is essential for each user; hence, this layer has direct communication with all the other layers mentioned above. The functions in this layer are responsible for providing authentication, confidentiality, access control, availability, and other security-related features. This is designed in such a way that the attacks or security threats can be minimized. This layer is liable for taking care of the security and privacy issues and to secure the network from any nonauthenticated access [24, 41]. Let us now take an example of communication in IoV architecture. As the vehicle starts, the engine state changes to RUN; it triggers the process of initialization of the vehicle and authentication with the network of IoV, and data acquisitions from the environment process started at that point in time. This acquisition step helps to collect all the required information produced by the vehicles, users, and roadside infrastructures such as traffic lights, location sensors for pollution level, and smart devices, within the flexible network area. Once the data is gathered, then it is filtered and preprocessed to make sure the significant data is transmitted to the driver who wants to get the information and discard the rest of the information which is not needed by the IoV network [7].

As an example, in case the vehicle receives the information on the accident, it displays on the infotainment panel to the driver, and its notification is being broadcasted. However, if any other vehicle receives a similar type of information without any change to it, then it stops rebroadcast for a second time. Based on the profile of the vehicle and the information available in the network, the best network is to be selected by using some routing-based algorithms. The set of protocols is managing the information which is being transmitted from the network to support the IoV environment as highly efficient for all the services. The information which is preprocessed is classified as private or business and sent to the cloud for analysis, process, and store and is available based on the type of the information.

Table 2 summarizes the comparison of the different IoV architectures proposed by the researchers in the past based on layered architecture, type of communication supported, and application type.

4. Protocols in IoV Communication

Compared to the VANET, the IoV works at a large scale, and the IoV system is quite complex, consisting of numerous heterogeneous network components and devices. Therefore, several technologies are required for IoV related applications to work [24, 33, 42, 43]. In the subsequent sections, a detailed description of the MAC layers and routing layers is explained. There are various routing protocols that are based on the topology and the position category. Section 4.1 elaborates the MAC layer protocols introduced by various researchers in the past few years [44, 45].

4.1. MAC Protocols. This section elaborates on the Medium Access Control (MAC) layer protocols. Mainly, the MAC layer protocols are based on IEEE 802.11 wireless communication. There is much research going on to develop MAC protocols for IoV, strictly on VANETs. Basically, a MAC protocol ensures the vehicle can send the received data packets that are non-safety related without impacting the safety-related messages sent during the high traffic density. There is an allocated frequency band for the vehicles by many of the countries. MAC protocols give instructions on how all the vehicles can access the channels in the VANETs. As in the VANETs, the change in the topology is frequent, and the vehicle moves at high speed, it is quite difficult to design the MAC protocols. The classification of the MAC protocols is basically done in three different categories: contention based, contention-free, and hybrid. In contention-based protocols, the vehicle which needs access for the channel competes for it, and after the access is granted, it can use the medium for a certain amount of time. The example is Carrier Sense Multiple Access (CSMA), as there are no boundaries on the delay; hence, the safety-related messages may not be guaranteed with this protocol. All the IEEE 802.11p protocols are based on CSMA protocols. On the other hand, in contention-free category, the access for the medium is preallocated.

All Wi-Fi standards belong to IEEE 802 local and metropolitan area networks, LAN, or MAN standards. All the Wi-Fi standards are part of the IEEE 802.11 series. At first, Wi-Fi standard was released in 1997, with no suffix added; however, as many more variants came into existence, a suffix letter was added to indicate the difference in those variants, which is lowercase. There are various standards under IEEE 802.11 that cover everything from network operators to interoperability, electronic security, access points, quality of service (QoS), roaming, and other required system elements. Table 3 illustrates the comparison of the different IEEE standards used in MAC. The major IEEE 802.11 standards are listed below:

IEEE 802.11a standard is the basic standard in IEEE 802.11 series. It defines a Wi-Fi format for providing wireless communication for raw data at a speed of up to 54 Mbit/s in 5 GHz ISM band. The performance of the 802.11a standard is impressive, capable of transmitting data

Table 2: Comparison of various state-of-the-art architectures for Internet of Vehicles (IoV) communication.

Reference	Year	Layers in proposed architectures	Functionality of layer	Communication supported	Simulation environment	Applications
[34]	2011	Three: client, connection, cloud	Client: helps to sense the information within and outside the vehicles Connection: helps to organize the route for the packets to be transferred in the communication Cloud provides the computing power and the revival of the information from the network	V2I, V2R, V2P, V2V	—	NA
[35]	2013	Four: embedded systems and sensors, multiservice edge, core, cloud	Embedded systems and sensors use the communication channel on 802.11p protocol for V2V communication Multiservice edge: helps to define the technology that enables communication between vehicles Core: helps in implementing information flow control strategies Cloud: it specifies the type of service needed and can receive the services	V2V	—	NA
[36]	2014	Three: vehicle computation, location computation, and cloud computation	Vehicle computation: helps in taking the context-aware systems for more contextual information which is related to the tasks while driving the vehicle Location computation: It is used by RSUs to exchange information with the vehicles in its range Cloud computation: Maintains the applications and the services.	V2I, V2V	MATLAB/Simulink	Parking reservation service
[20]	2016	Five: perception, coordination, artificial intelligence, application, and business	Perception: works on the physical layer protocols with the help of the 802.11p series Coordination: helps to provide secure transmission Application: statistics and services are performed on this layer Artificial intelligence: decision-making and the processing of the data done at this layer Business: helps to provide the models, budget preparation, and the aggregation of the data	V2I, V2R, V2P, V2S, V2V	—	Traffic safety, infotainment, web-based utility
[18]	2016	Three: area network, network management, and device to device applications	Area network: many devices connect and gather the data at this layer Network management: supports management in a distributed manner Device to device applications: Based on the degree of involvement of the base station, it helps communicate between the devices. Business: Holds the private cloud, public cloud, and enterprise cloud.	V2V	MATLAB	Video-related

Table 2: Continued.

Reference	Year	Layers in proposed architectures	Functionality of layer	Communication supported	Simulation environment	Applications
[37]	2017	Seven: user interaction, data acquisition, preprocessing, communication, management, business, security	User interaction: acts as notification management for the communication Data acquisition: deployed with all the intravehicular and intervehicular communication Pre-processing: transmission, preprocessing, and filtering functions are the significant responsibility of this layer. Communication: provides the services with the help of various technologies like Wi-Fi, LTE, 3G. Management: inspection of the data packets, management based on the flow of data are the responsibility of this layer. Security: linked with all the layers to provide the authentic, authorized, trust, and privacy on the data	V2I, V2R, V2P, V2S, V2V	—	Traffic efficiency-related
[32]	2019	Three: client level, connection level, cloud level	Client level: helps in communication between the vehicles Connection level: all the control stations and the radio access units are deployed at this layer Cloud level: act as a backbone of the architecture and supports the communication with the help of network/internet	V2I	NCTUns 6.0, OPNET Modeler	Congestion control
[38]	2019	Three: t1, tier 2, tier 3	Tier 1: connects with the cloud server and consists of the components like cloud network and servers Tier 2: the RSUs and the access point are being deployed at this layer Tier 3: contains the information on the sensors and the actuators	V2V, V2I	Vehicular Network Open Simulator	NA
[39]	2020	Four: data collection, network, data processing and knowledge discovery, application	Data collection: gathers the data from the numerous heterogeneous devices present in communication Network: it accommodates the connection of the devices with the help of wireless access networks Data processing and knowledge discovery: data management and batch processing is done here. This layer also performs the data mining with the support from artificial intelligence and machine learning techniques Application: all the applications are being managed in this layer	V2V, V2I	OMNET++	Public transport, social transportation, traffic management, regional logistics management, telematics, fleet management, and parking management
[40]	2020	Three: mobile user, MEC, cloud	Mobile user: interacts with the vehicles MEC: helps to load the data to the MEC servers received from RSUs Cloud: manages the core network of the communication	V2V, V2I	—	Safety-related

Table 3: Comparison of IEEE MAC standards for Internet of Vehicles (IoV) communication.

Parameters	IEEE standards							
	802.11a	802.11b	802.11g	802.11n	802.11ac	802.11ad	802.11ah	802.11ax
Standard approval date	1999	1999	2003	2009	2013	2016	2017	2021
Maximum data rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	6.93 Gbps	7 Gbps	347 Mbps	9607.8 Mbps
Modulation technique	OFDM	CCK (DSSS)	CCK, DSSS, OFDM	CCK, DSSS, OFDM	BPSK, QPSK, QAM,	Single carrier and OFDM	MCS	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM
RF band in GHz	5	2.4	2.4	2.4/5	5	60	0.9	2.4/5 6 GHz for Wi-Fi 6E
Width of channel in MHz	20	20	20	20, 40	20, 40, 80, 160	—	1	20, 40, 80

at speeds of up to 54 Mbit/s, which was considered a good range. But in the scenarios like video transmission where the data rate need is high, it could not provide the maximum data rate [46]–[47]. IEEE 802.11b was the first widely used WIFI standard, and it operates in the 2.4 GHz band. The development of this technology is easier and cheaper than 802.11a, which has a higher 5 GHz frequency band. 802.11b is built into many laptops and other hardware, which cements its success. For data transmission, 802.11b uses the CSMA/CA method, defined in the original 802.11 basic standards and reserved for 802.11b. Using this method, when a node wants to send the data, it listens on the idle channel before transmitting and then waits for confirmation. If no confirmation is received, the random waiting time is assigned, assuming another transmission is taking place. If it gets interference, then, it listens to the free channel and then forwards the data [46–49].

IEEE 802.11g is one of the main Wi-Fi standards that follow 802.11a and 802.11b. It is built for high performance and helps make Wi-Fi the main wireless standard. The advantage of IEEE 802.11g is that it can support high 2.4 GHz data rates, which can only be achieved by using 802.11a in the 5 GHz ISM band. Like its predecessor, 802.11b, 802.11g works in the 2.4 GHz ISM band. It provides a maximum raw data throughput of 54 Mbit/s, although this means that the actual peak throughput is just over 24 Mbit/s [46]–[47]. IEEE 802.11n is proposed next in the IEEE 802.11 LAN series after 802.11a, 802.11b, and 802.11g to meet the demands of Wi-Fi technology for higher speed and capacity. With the higher data rates usually driven by video, IEEE hopes to stay ahead and ensure that Wi-Fi can meet users' needs in the coming years. In early 2006, the industry reached a large consensus on the 802.11n wireless LAN system specifications, which provided enough information for many chip manufacturers to begin their designs. The draft was completed in November 2008 and officially published in July 2009 [46–49].

IEEE 802.11ac was proposed to further increase the speed of wireless local area networks and the communication speed between smartphones, Wi-Fi-enabled TVs, game consoles, and many other Wi-Fi-enabled electronic devices. The minimum VHT data rate is at least 1 Gbit/s, and the maximum is 7 Gbit/s. At this order of speed, WLAN or general wireless connections can operate and LAN or Wi-Fi and not be the limiting factor [46]–[47]. IEEE 802.11ad, also called as WiGi or Gigabit Wi-Fi. This protocol is to provide extremely high bandwidth data and uses millimeter-wave frequency bands where high bandwidth is required. IEEE 802.11ad is defined as the Multiple Gigabit Wireless System (MGWS) standard and can operate at up to 60 GHz frequencies. Due to the use of very high frequencies, the range is limited, usually only a few meters, and is blocked by walls. WLAN and general wireless connections can operate without LAN or Wi-Fi as the limiting factor at this order of speed. Although the 2.4 GHz and 5 GHz bands are mostly used for Wi-Fi, some ISM allocations are below 1 GHz. IEEE 802.11ah is designed to use an unlicensed spectrum below 1 GHz. One of the advantages is that it can provide a better communication range. Therefore, it supports the Internet in all aspects [46–49].

IEEE 802.11ah is a Wi-Fi standard designed towards use unlicensed ISM frequency bands below 1 GHz. The propagation of radio communication on these frequency means that signals can travel long distances, which opens opportunities for the Internet of Things. The frequency bands of these frequencies are much smaller than the 2.4 GHz and 5 GHz frequency bands commonly used in WLAN, which limits the data transmission rate on the channel [46]–[47]. IEEE 802.11ax is established in accordance to the IEEE 802.11 series, which is also called Wi-Fi 6. Compared with 802.11ac, there is a significant improvement, especially in dense deployment, spectrum efficiency, and user access. IEEE 802.11ax is aimed at improving user-friendliness and is considered the successor of 802.11ac. The new 802.11ax is still in the emergence of development, but it is four times faster than IEEE802.11ac [46–49].

4.2. Routing Protocols. When communication comes into the picture, the routing protocols play a significant role. Routing is the responsibility of the network layer which ensures optimal path selection from source to destination in the IoV network. Generally, the broadcasting technique is being used, but still, there are applications that support unicast communication. Routing in IoV is different from the routing in MANET as the nodes are moving at high speed, and there exist constraints such as huge buildings, trees, and other signals that interrupt the routing process [14, 50, 51]. So, it is essential for any of the applications to have good routing protocols to have a minimal E2E delay and a good PDR. The researchers are working on the routing protocols that ensure a good delivery ratio and minimum packet loss. The routing approaches are basically categorized as proactive, reactive, and hybrid. A proactive approach requires maintaining the topological information of other nodes present in the networks regardless of whether the nodes are participating in the communication. It is also known as the table-driven approach. Since proactive protocols store all topology information in advance for the nodes in the routing table, it has low latency but more network.

In contrast to the proactive protocol approach, a reactive protocol approach computes the routing information to a destination only on demand basis. So, as a result, the network overhead is low. The issue with the reactive method is that if the network is disrupted due to the frequent movement of the vehicles, it takes a longer duration to compute and establish the routing path from a source to a destination. A hybrid routing scheme combines the benefits of proactive and reactive routing. The routing is initially set up with a specific proactively approach, and then, reactive flooding fulfills the demand to find the path from source to destination. Hence, it is well suited for low and high traffic loads.

In IoV, the routing protocols are classified into two categories: topology-based and position-based. In topology-based protocols, it is necessary to maintain the routing table to forward the packet from a source to a destination. In IoV, because of the higher mobility, the change in the topology is very frequent; therefore, topology-based protocols are not much suited in IoV due to large network overhead and delay. However, in position-based protocols, there is no need

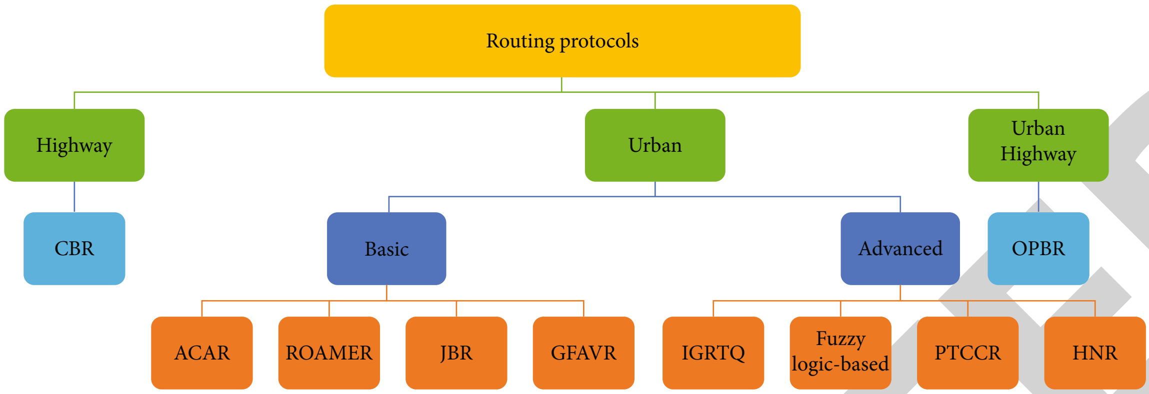

FIGURE 5: Taxonomy of Internet of Vehicles routing protocols based on environment type for highway and urban scenarios.

to maintain the table to form a network from source to destination since it utilizes the greedy or carry and forward approach to send the packet from source to destination. Hence, position-based routing protocols are preferred over topology-based routing in IoV.

The environment considered for position-based routing protocol is either urban or highway. The highway environment majorly consists of straight routes. It is observed in highway scenarios that the packet delivery ratio is quite good. The urban area consists of buildings, streets, trees, and malls. These environmental factors influence various performance metrics for the routing, including packet deliver ratio, routing overhead, and end-to-end delay, so it is highly recommended to develop protocols which are well suited for the urban environment.

An illustration of an important state-of-the-art IoV routing protocol based on environment type is given in Figure 5, and the same description is elaborated in this section.

4.2.1. Adaptive Connectivity Aware Routing (ACAR). Adaptive Connectivity Aware Routing (ACAR) [52] uses the real-time density of the nodes. This protocol is based on choosing the opportunistic path considering the network quality for transmission of the data packets. This presumes that all vehicles are preloaded with GPS maps that contain all the information of the vehicle density, number of vehicles, and path information. The ACAR protocol works in the two main phases: optimal path selection and an efficient way to increase the packet delivery ratio. Generally, the optimal path is selected by taking transmission quality models into consideration and the traffic light estimation. The destination receives the request from the source; if the statistical difference is high, then the destination asks the source to select some other path to send the data packets, as shown in Figure 6. The ACAR protocol's major disadvantage lies in the lack of information about the destination's location if the map gets crashed.

4.2.2. Cluster-Based Routing (CBR). It is a cluster-based routing (CBR) [53] protocol that utilizes the geographical area into the clusters. Every cluster has the cluster head and an Identifier (ID) which is usually the MAC address. The cluster head broadcasts its availability to the network; then, the neighboring nodes acknowledge the cluster head to join the cluster network. If the cluster head needs to leave the responsibility of broadcasting, it triggers a message to all the cluster nodes about its unavailability to be a part of a cluster. If a start node wants to send the packet to the final node, it then sends the data packets to other nodes present in its cluster range towards the destination. CBR has good performance, and the packet delivery ratio is quite high as compared to Destination-Sequenced Distance-Vector Routing (DSDV) protocol. The major disadvantage of using the CBR approach is that when the cluster head cannot find any nearer nodes, it drops the packets that might lose critical information.

4.2.3. Roadside Units as Message Routers (ROAMER). ROAMER makes use of the existence of RSUs to deliver the data to remote area in VANETs beyond undoubtedly knowing the position of the vehicle [54]. In order to protect the privacy of vehicle identification, vehicles use pseudonyms as a substitute of their real identities when communicating. Therefore, the start node "SN" requesting to send the data packet "DP" to the remote node "RN" can send the data packet to the nearest RSU (RS1) (if R1 exceeds its transmission range, the shortest path algorithm is used), and then the packet "DP" to the next RSU (RS2) through the backbone network. R2 can use multihop technology to send packets to "RN."

4.2.4. Junction-Based Routing (JBR). This approach uses the greedy-based selective routing for the nodes present at the road junction and closest to the destination. The minimum angle method is proposed as a recovery strategy if the maximum local problem is encountered, regardless of the relative position of the initial node, final node, and the intermediate nodes present in the network. JBR outperforms in packet delivery ratio and E2E delay compared to the traditional protocol Greedy Perimeter Coordinator Routing (GPCR) [55]. This protocol is based on the V2V communication and applies to urban areas.

4.2.5. Greedy Forwarding with Available Relays (GFAVR). GFAVR is designed for the Crowd Sensing Vehicle Networks (CSVNs). Considering the local maximum problem

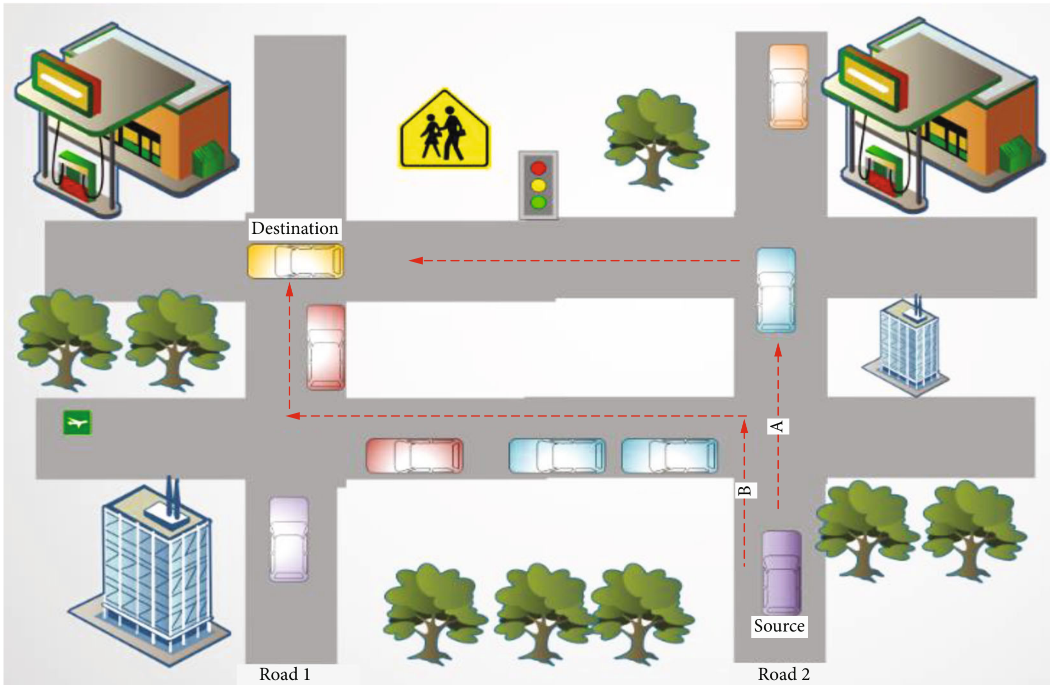

Figure 6: Communication mechanism of Adaptive Connectivity Aware Routing in IoV.

in the greedy approach, the proposed protocol shows an improvement of data delivery by 10-40%. The simulation is performed on the urban scenarios, and there is no preliminary phase involved, but the protocol is fully distributed. When any RSU does not cover the OBU and there are no neighboring nodes available to forward packets, then the OBU itself broadcasts its unavailability as a relay node. Therefore, the neighboring vehicles will not consider this OBU as a possible next relay. The proposed protocol is simpler and fully distributed and needs not consider any prior knowledge of the scenarios [56].

4.2.6. Intersection-Based Geographic Routing with Transmission Quality (IGRTQ). IGRTQ is applicable to the urban VANETs scenarios. To select the most suitable route, each road is allocated with a weight. The information about the connections of the roads and the delay is the parameters to calculate the weighting parameters for various available routing paths in the network. Information received from these weights helps to select the routing path. It sends the beacon packets to know the current position of node. Due to high mobility, the chances are that sometimes when node sends the data then other node may be out of transmission range, which means that the routing used to navigate the data packet is incorrect. The data transmission link is good in road 2 as shown in Figure 7. However, in the case of road 1, the source and destination are beyond 250 m of transmission range but still following this protocol, multihop transmission can take place, and it is possible to send the data packet on the road 1. This protocol outperformed in packet delivery ratio when compared to the Greedy Perimeter Stateless Routing (GPSR) [57] and Junction-Based Routing (JBR) protocol.

4.2.7. Fuzzy Logic-Based Geographic Routing. It is based on fuzzy logic and vehicle to vehicle communication in urban areas [58]. This protocol takes the direction, the quality of the link, and the available bandwidth into consideration while sending the packets from the initial node to the final node. In this approach, link quality estimation is determined by the expected transmission count metric. Apart from this, the Fuzzy logic protocol also takes the highest throughput path into consideration while selecting the next hop for the transmission of a data packet in the network. It uses a carry and forward strategy if there is the unavailability of neighbor nodes until the new neighbor is available to receive the packet.

4.2.8. Path Transmission Cost-Based Multilane Connectivity Routing (PTCCR). In PTCCR, routing decision occurs by using the intersection nodes or via the neighbor nodes [59]. This approach investigates the connectivity in the multilane's areas based on the vehicles' speed at the different road sections. The transmission cost of a path is measured to incur the minimum cost required to travel the packet. Upon estimation of the cost of transmission from a route, the optimal path selection process takes place. The optimal path selection process also considers various other parameters, including multilane connectivity, lowest transmission cost, transmission direction, location of the neighbor, and position of the destination. Simulation results showed that PTCCR outperforms better than traditional protocols in terms of PDR and the minimum E2E delay.

4.2.9. Opportunistic and Position-Based Routing (OPBR). OPBR uses a greedy approach scheme from the initial node to the destination node based on the greatest geographic area

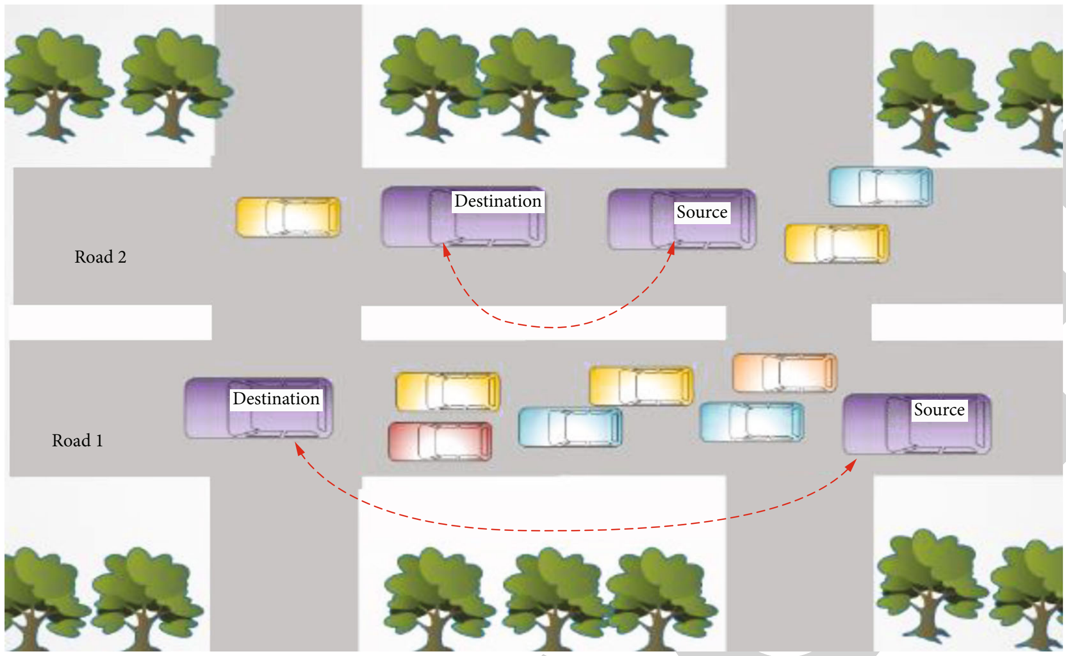

Figure 7: Communication mechanism of Intersection-based Geographic Routing with Transmission Quality for IoV.

so that there shall be the least number of hops between the transmissions for the data packets [60]. This approach or protocol selects the optimal candidate node and then regulates the priority for data transmission. This protocol is based on the greedy forward strategy applicable for V2V communication on the urban and highway regions.

4.2.10. Reliable Hybrid-Network-Oriented V2V Data Transmission Routing (HNR). HNR is based on the Manhattan mobile model. This protocol considers the RSUs as wired and wireless mediums of data transmission. It utilizes a probabilistic model that keeps a constant check on the vehicle's connectivity with the help of RSUs. Integration of V2V and V2R communication is proposed to improve the quality of the data transmission. Simulation results exhibit that the HNR outperforms concerning the packet delivery ratio and minimum number of average hops required to send the packet from source to the destination as compared to traditional [61].

4.2.11. SURFER: A Secure SDN-Based Routing Protocol for Internet of Vehicles. ROAMER is upgraded by moving routing activities to the SDN. As a result, researchers offer a routing protocol for the IoV which is called as SURFER that routes packets safely and effectively using a Blockchain system and a distributed SDN architecture within the RSU network. SURFER-1 and SURFER-2 are proposed which are SDN-based, assuming that the IoV is divided into RSU clusters, that each RSU cluster contains an SDN cluster controller, and that the cluster controllers are linked to an SDN main controller. SURFER-1 only implements SDN operations within the RSU network, whereas SURFER-2 employs SDN-based routing procedures across the entire IoV. To secure the proposed protocols, researchers presented a blockchain model that uses the HPBC algorithm to create and maintain two blockchains: a Routing Blockchain and a Data Blockchain. The authors described the simulations to test the performance of the two proposed protocols. They illustrated the comparisons made with two existing IoV protocols: Quality of service-aware Routing Algorithm (QRA) and SDN-enabled routing for IoV (SD-IoV). The simulation results showed that SURFER is more efficient than other IoV routing protocols in terms of latency, packet delivery, and network overhead [62].

4.2.12. Advanced Greedy Hybrid Bio-Inspired (AGHBI). To improve the performance of IoV, an Advanced Greedy Hybrid Bio-Inspired (AGHBI) routing protocol is proposed. The protocol is based on the greedy forwarding system, in which a modified hybrid routing scheme using a bee colony optimization is used that helps to select the route with the highest quality of service and maintains the path with the least amount of overflow. AGHBI employs two basic steps: first, a greedy scheme to forward the packets is utilized to select the nearest destination, followed by a modified hybrid routing system that uses an ABC optimization algorithm to choose the most significant QoS route and preserve the path with the least amount of overflow. The simulation results show that the AGHBI protocol is suitable for the large urban and highway scenarios, outperforming in PDR by 13.9% and 29.7% when compared with AODV and GPSR protocol. The simulation results also shows that the AGHBI works well with both V2V and V2I environments. It significantly impacts PDR and delays while maintaining minimum hop count across all vehicles [63].

4.2.13. Mobility Aware Dynamic Clustering-Based Routing (MADCR). The IoV is an enhancement of IoT that enhances the capabilities of VANETs in ITS. The authors propose the MADCR protocol in IoV to increase network longevity and decrease the packet delay. The formation of cluster and cluster head (CH) selection is a major part of the MADCR process. The network's clusters are formed using Euclidean distance. The mayfly optimization algorithm MOA is then used to choose the CH. Finally, the CH gathers data from the vehicles and sends it to the RSU that has access to the Internet. MADCR protocol's performance is compared to that of Comprehensive Learning Particle Swarm Optimization (CLPSO), Ant Colony Optimization (ACO), and Clustering Algorithm for Internet of Vehicles based on Dragonfly Optimizer (CAVDO). It was suggested that MADCR methodology boosts PDR by 6%–16% while decreasing latency by 6–100 ms in real-time scenarios [64].

4.2.14. Heuristic Routing for Vehicular Networks (HERO). The authors developed HERO, a distributed routing protocol for the vehicular urban environment, including two heuristic functions to optimize the selection of road segments and vehicles on-road segments. The Interpath was created to choose a route path comprised of numerous road segments with reduced distances and higher connection networks. It was accomplished using two probability distributions, the Shortest Distance Distribution (SDD) and the Connectivity Distribution (CD). Each distribution considers various values that represent the physical quality, which improves the routing choice. SDD takes the direction angle, perpendicular distance, and segment length, whereas CD takes into account the communication range, lane count on the road segment, segment length, and predicted vehicle count.

Although considering the fact that the technique of multicriteria routing may significantly improve the performance of VANET, two significant obstacles are encountered when working on this research. The first issue is determining how to mathematically describe each criterion, while the second is determining how to combine these conflicting criteria to arrive at an optimal routing option. HERO enables V2V communication, but it may be upgraded to support V2I communication by permitting vehicles to pass packets to RSUs at junctions instead of searching for a forwarder vehicle on another adjacent road segment [65].

4.2.15. Traffic Aware and Link Quality Sensitive Routing Protocol (TLRP). In this research, the authors suggest an IoV protocol based on intersection routing with traffic awareness and link preference. TLRP protocol seeks the optimal routing path in between two communication nodes with the maximum PDR and least transmission delay. A new routing measure Link Transmission Quality (LTQ) that takes both transmission cost and forwarding reliability into account is first designed, which uses the influence of the relative locations of the connections along the routing path on network performance. Each road segment is allocated a distinct weight based on the intended LTQ using the newly implemented intersection backbone nodes. Finally, the routing path with the lowest summed LTQ is chosen as a candidate for data transmission. Two data transmission algorithms for packet forwarding are used to deal with the enormous scale of modern cities. In terms of PDR and E2E delay, simulation results reveal that the proposed protocol beats existing routing methods. More network performance effect elements, such as the number of retransmissions and average transmission hops, will be included in the future work during routing metric construction and path selection [66]. Table 4 illustrates the comparison of IoV routing protocols.

5. Experimental Analysis

For a comparative study in this manuscript, the comparison between PTCCR, HNR, and OPBR has been performed. The execution is performed using existing protocols on the network simulator NS 2. The five repetitive simulation rounds for every varying packet sizes and the average reading of these simulation rounds are considered and shown through graphs. The other simulation factors used are also summarized in Table 5. The PDR is equal to the ratio of data packets delivered to the destination node successfully to the total number of packets transmitted from the source node. In Figure 8, the results exhibit a better PDR approximately 98%, when the number of nodes taken for the simulation is 300, which is highest in comparison with HNR and PTCCR protocol. The PTCCR also shows 80% of the PDR when vehicles are 100.

The end-to-end delay is also an utmost QoS parameter that calculates the average time interval between receiving and sending a packet from a source to destination nodes. In Figure 9, the HNR performs better in the simulation parameters than other protocols, OPBR and PTCCR, in the case of E2E delay when the number of vehicles is high. Results show that when the number of nodes is 300, then the E2E delay observed for the HNR is approx. 0.5 seconds, whereas in OPBR, it is 0.65 seconds and, in PTCCR, it is 0.89 seconds. The application related to safety must have a minimal end-to-end delay so that the packet reaches from the source to the destination well in time without much delay.

Majorly, IoV's routing protocols follow the greedy-based approach; once the local maximum is reached, the packets start dropping, and it results in a PDR. Therefore, it results in a lower packet delivery ratio. The simulation results exhibit that the HNR protocol has the highest packet drop ratio, which is approximately 30% in comparison with PTCCR and OPBR, which is 10% and 2%, respectively, when the number of vehicles is 300 as shown in Figure 10. Hence, the HNR protocol is not considered the best fit for the safety-critical application but can be used for other infotainment-related applications.

6. Summary and Discussion

Below is the summarization and discussion on the overall IoV architecture and protocols discussed in this paper.

6.1. Summary of IoV Architectures. The three-layer architecture proposed by Liu supports V2V, V2I, V2P, and V2R communication. Many researchers have taken this as the base architecture initially for their research on IoV architecture. However, this does not include the application of V2S

Table 4: Comparison of various state-of-the-art routing protocols for Internet of Vehicles (IoV) communication.

Reference	Protocol	Forward strategy	Repair strategy	Map required	Environment	Communication type
[52]	ACAR	Greedy	Carry and forward	Yes	Urban	Unicast
[53]	CBR	Cluster based greedy	None	No	Highway	Cluster
[54]	ROAMER	Geographic location	Carry and forward	Yes	Urban	Multicast
[55]	JBR	Selective greedy	Minimum angle	Maps	Urban	Broadcast
[56]	GFAVR	Greedy	Carry and forward	Yes	Urban	Broadcast
[67]	IGRTQ	Greedy	Adaptive intersection strategy	Yes	Urban	Broadcast
[58]	Fuzzy logic-based protocols	Fuzzy logic	Carry and forward	Yes	Urban	Broadcast
[59]	PTCCR	Farthest neighbor	Carry and forward	Yes	Urban	Unicast
[60]	OPBR	Greedy	Unknown	Yes	Urban, highway	Broadcast
[61]	HNR	Greedy	Distance and angle	Yes	Urban	Broadcast
[62]	SURFER	Geographical and carry-and-forward	Geographical and carry-and-forward	Yes	Urban, highway	Broadcast
[63]	AGHBI	Greedy	Back up path	Yes	Urban, highway	Multicast
[64]	MADCR	Cluster based greedy	Unknown	Unknown	Urban	Cluster
[65]	HERO	Direction and carry-and-forward	Unknown	Yes	Urban	Broadcast
[66]	TLRP	Link Transmission Quality	Unknown	Yes	Urban	Broadcast

Table 5: Simulation parameters.

	Simulation parameters	
S. no.	Parameters	Value
1	Simulation area	2000 m ∗ 2000 m
2	Range	250 m
3	Speed minimum	30 km/h
4	Speed maximum	60 km/h
5	Hello interval	1 s
6	Traffic flow	Free-flow
7	Packet size	512 bytes
8	MAC protocol	IEEE 802.11 p
9	Number of nodes	100,150, 200,250, 300

like OTA so that the vehicles can communicate to the servers; hence, the V2S communication is not supported via this IoV architecture. To support V2V communication, there is another architecture of IoV proposed by Bonomi et al., which has four different layers. This proposed architecture does not support V2R, V2P, V2S, and V2I. Therefore, further improvements are required to be incorporated to provide full support for IoV communication. Wan et al. described the three-layer architecture for IoV considering the communication between the V2V and V2I. This architecture considers only VANET communication, whereas future enhancements are required in this architecture so that the other aspects of IoV communication related to the servers, pedestrians, etc. can be explored. Kaiwartya et al. proposed the five-layer architecture of IoV that can cover the IoV aspects in terms of the IoV communication and the applications supported. However, this has few limitations concerning security and cyberattacks.

The architecture proposed by Gandotra et al. supports V2V IoV communication. This architecture has three layers. The security concerns also have been addressed by the author related to V2V communication. However, this IoV architecture needs to be reworked considering the dense traffic conditions on the roads. Contreras-Castillo et al. described the seven-layer architecture of the Internet of Vehicles; this architecture is based on all IoV communication and considers all the aspects of security with every layer.

Sherazi et al. proposed a V2I-related IoV architecture based on the heterogeneous network to transmit the data. A future work on this architecture requires covering the cost-effectiveness and the classification of the vehicles based on the other IoV applications. Tolba and Altameem proposed the three-layer architecture of IoV considering the V2I and V2V communication. The architecture is divided into three layers named tier 1, tier 2, and tier 3. Future enhancements are required to extend the authentication of the vehicle on the message's level. Arooj et al. proposed the four-layer architecture which supports the V2I and V2V communication. The architecture is proposed considering the optimal route selection using 5G technology, and it supports only VANET communication; however, this architecture can be extended further for IoV communication. Ji et al. proposed three-layer architecture based on mobile edge computing and cloud computing. This is established to

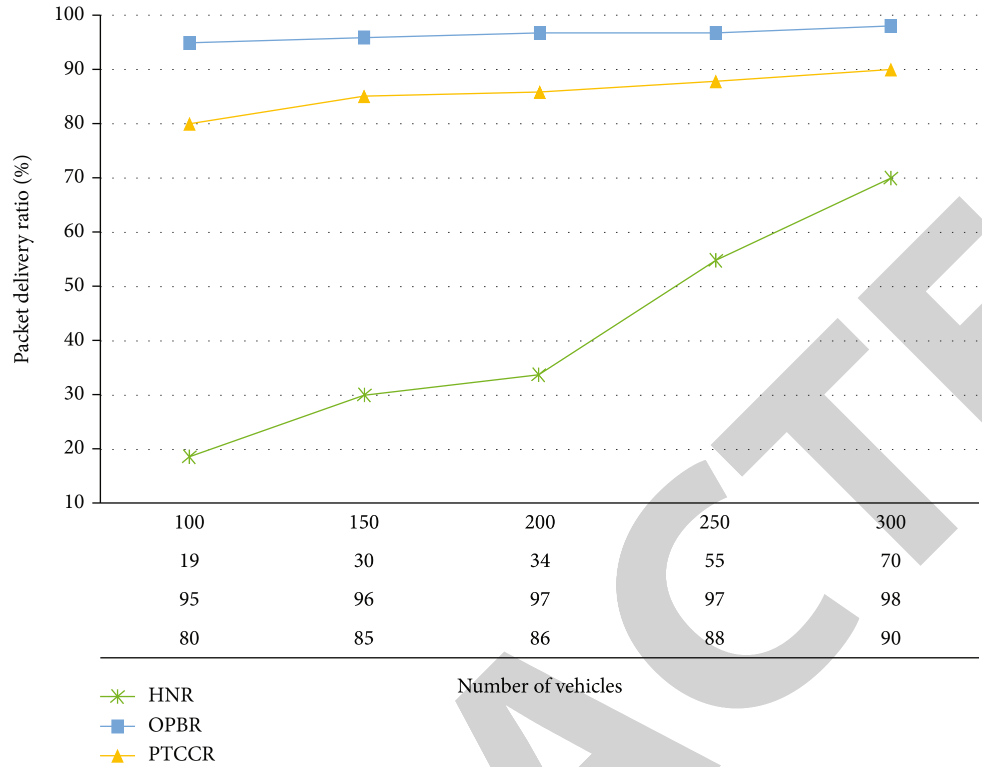

Figure 8: Comparison of packet delivery ratio with the number of vehicles.

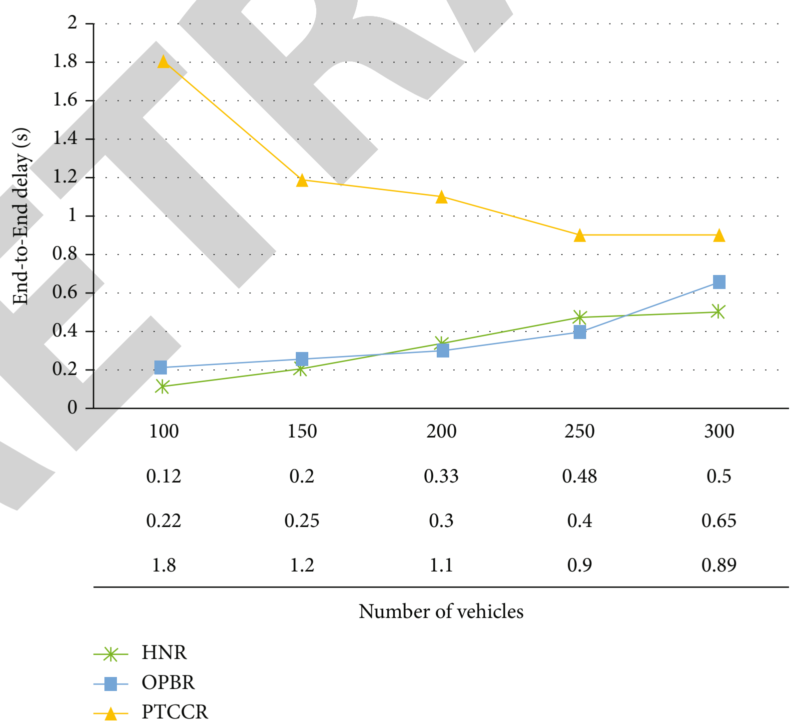

Figure 9: Comparison of end-to-end delay with the number of vehicles.

support the V2I and V2V communication and the cloud interaction with the vehicles. The authors have combined the applications of AI and MEC to the IoV and provided the analysis results. Also, future challenges have been discussed related to noncooperative and cooperative caching. Figure 11 depicts very few architectures present that support

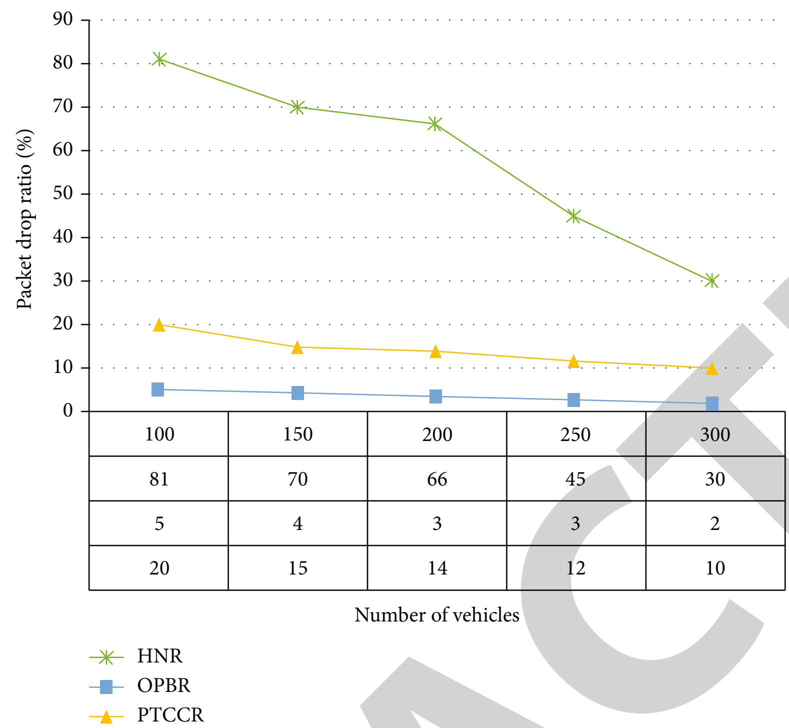

Figure 10: Comparison of packet drop ratio with the number of vehicles.

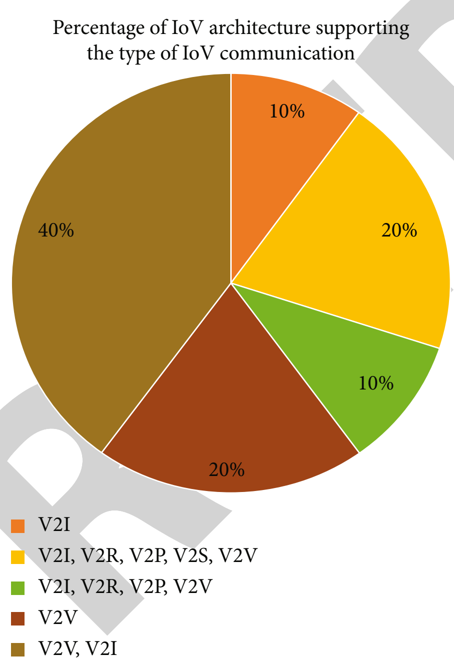

Figure 11: Percentage of IoV architecture supporting the IoV communication types.

all types of communication in the IoV. Hence, there is a need to explore the architecture for all communication types.

6.2. Summary of MAC Protocols. Several protocols based on IEEE standards have been proposed at different time intervals. Comparison has been made between the most used protocols in IoV IEEE 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, 802.11ad, 802.11ah, and 802.11ax, based on the maximum data rate and modulation techniques supported. The IEEE standard 802.11b supports the maximum data rate up to 11 Mbps with frequency modulation of CCK (DSSS). However, the 802.11ad supports the maximum data rate of 7 Gbps with a single carrier and OFDM frequency modulation. Even though a special MAC protocol series has been developed for the IoV, exclusively in VANET, the multihop communication in the IoV is still a challenge due to high speed of vehicles and poor communication. Researchers are paying more and more attention to this topic; specifically, using vehicle-friendly mechanisms to forward messages at the network layer is very alluring, including broadcast-based distribution and messaging using unicast. Still, the extensively used protocols are not yet available.

6.3. Summary of Routing Protocols. ACAR protocol is used in the urban scenario for IoV communication, but if the map crashes, the nodes do not have any information of the location of the destination node. Therefore, further enhancements are required to provide the routing information in case of failure of the map. CBR protocol is applicable for highway scenarios and does not need the maps before the vehicles. It usually uses the cluster head ID with the MAC address to find the next node towards the destination. However, when the cluster head cannot find any nearer nodes, it drops the packets that may lose the critical routing information. ROAMER supports the position-based routing that utilizes a carry and forward approach to forward the data packets. In this approach, RSUs act as a messenger; it supports V2I communication. However, future improvements are essential for the delay-tolerant behavior to support safety-related applications. JBR is applicable in the city scenarios, especially while selecting the optimal routing path at the junction nodes present at the junctions. The coordinator nodes near the junction are supposed to pass the packets toward the destination. The protocol uses the selective greedy approach and the minimum angle method in case of recovery from the maximum local condition. It is a non-delay tolerant protocol; hence, it is best suited for security and safety-related applications.

GFAVR is based on the V2I communication for urban scenarios, and it follows the greedy approach to forward the packets. This protocol shows high scalability in terms of the area taken into consideration for the simulation. The results exhibit that it has a good PDR as compared to the GPSR. IGRTQ utilized the greedy forwarding and adaptive selection strategy. It considers only V2V communication and lacks the scalability factor. Therefore, future enhancements are needed to upgrade the scalability of the protocol. Fuzzy logic-based protocol proposed is based on broadcast communication, and fuzzy logic selects the next node from the source to the destination. It is best suited for urban scenarios and utilizes the carry and forward approach for IoV communication.

PTCCR is applicable for the urban scenarios in IoV communication. While routing, it selects the farthest node as a next-hop to minimize the number of hops to reach the destination node. It exhibits a good packet delivery ratio and end-to-end delay, hence suited for efficiency and safety-related applications. HNR is applicable to urban scenarios and is based on the data transmission of Manhattan mobility. It integrates the V2I and V2V communication, performs well in case of the minimum hops taken towards destination, and shows a good packet delivery ratio. OPBR protocol is employed in urban and highway scenarios, and it exploits opportunistic and position-based schemes. OPBR has provided good results in terms of the packet delivery ratio and end-to-end delay. But it is observed that with the increase in the vehicle's speed, the packets start dropping. Hence, mobility of vehicles at high speed is still an area to be explored. SURFER is an IoV protocol which is an enhanced version of ROAMER. It applies to both urban and highway scenarios. The higher network traffic overhead is observed in this protocol, which needs to be improved, further.

AGHBI applies to urban and highway scenarios and utilizes the greedy approach to choose the nearest segment. It resulted in a better PDR when compared to the traditional GPSR protocol. Still, it is required to test this protocol on the complex IoV scenarios. MADCR supports the position-based routing that utilizes a cluster-based greedy approach to forward the data packets. In this approach, the latency is reduced as it uses the Euclidean distance for the cluster selection. However, future improvements are essential for highway-related scenarios. HERO is applicable for urban scenarios. While routing, it broadcasts the data packets for the next-hop selection to reach the destination node. It exhibits a good packet delivery ratio and end-to-end delay. Hence, it is suited for efficiency and safety-related applications. It is applicable for V2V communication, whereas V2I is an area to be explored further. TLRP protocol is employed in urban scenarios, and it exploits the link transmission scheme. TLRP has provided good results regarding the packet delivery ratio and latency. Further, it is observed that the protocol should consider QoS-related performance parameters for future enhancement. Figure 12 depicts trend that there are very few protocols present that support both the highway and urban scenarios in IoV communication. Hence, there is a need to research the suitable protocols for both the highway and urban environments.

7. Characteristics, Applications, and Challenges of IoV

The below mentioned section elaborates the characteristics of IoV, discusses numerous applications supported by IoV communication and the challenges in this domain.

7.1. Characteristics. The IoV network is majorly a combination of vehicle nodes, which tends to behave asymmetrically from the wireless nodes present in Mobile Ad-hoc NETwork (MANET). Therefore, multiple characteristics may affect the implementation and layout of the IoV environment. In variation in the communication environment, the automotive networks are primarily managed in the two typical communication environments. The traffic of highway scenarios is relatively straightforward, with no significant obstacles on the road. For example, the movement is in one direction, whereas it becomes much more complicated in urban scenarios. Streets in the urban areas are generally divided by the homes, construction places, infrastructures, trees, and other interruptions; therefore, it is not feasible to have a straightforward way of communication in that order of direction. Hence in IoV, the urban areas and the streets associated are considered while developing the IoV routing protocols so that the PDR achieved is better than the traditional protocols present [53].

In efficiency and repository, the significant characteristics of vehicles in the IoV environment are that vehicles have a plethora of energy and capability for the computation that includes the storage and processing, as nodes are vehicles rather than any phone devices carried with hands. Hence, the computation on the directions and the speed needs to be considered in the IoV environment [54, 55, 68]. In predictable mobility, the vehicular network is quite different from other types of ad hoc networks because the vehicles are generally moving with high speed and in any direction. Vehicles depend on terrain and street planning and the requirements for receiving traffic lights from signals and consider the distance to other moving vehicles, which makes their mobility predictable. So, it is expected to have inbuilt GPS systems in a vehicle to know about the mobility of the vehicles [69]. In geographical communication, the vehicular network consists of communication that needs to consider the topographical location. The actual data needs to be sent in case of safe-driving applications compared to other networks where the destination uses unicast or multicast for communication. The IoV supports security applications with minimal end-to-end delay and less possibility of packet loss [20, 70].

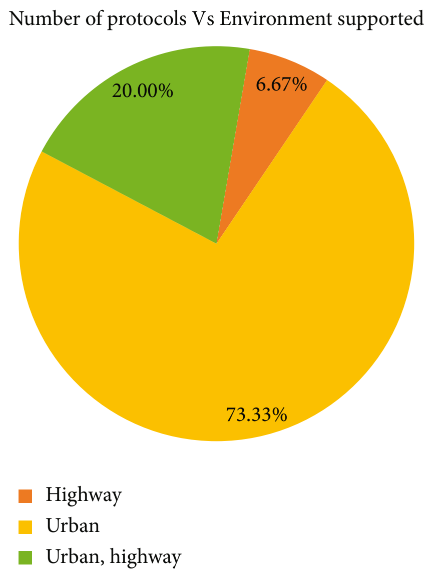

Figure 12: Protocols supporting the different communication environment in IoV.

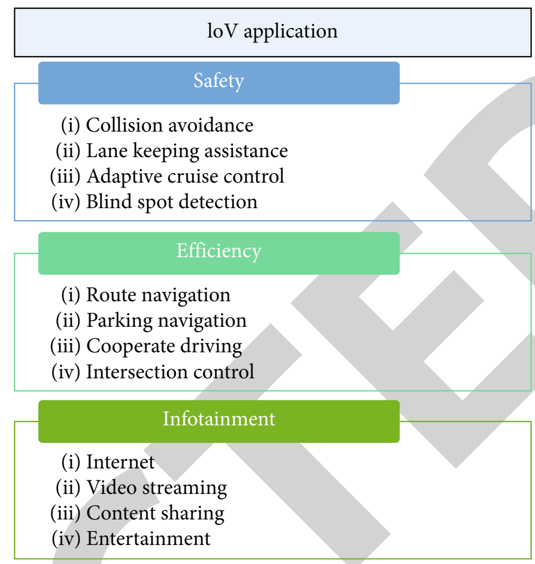

Figure 13: Applications based on the Internet of Vehicles (IoV).

In a large-scale network, the significant characteristic of the IoV is that the network is dense as it considers the features like streets, urban areas, highways, entrances to big cities, monumental buildings, city centers, and forests. Several protocols are based on the streets, and junctions have been proposed by many of the researchers. Also, the obstacles like building, forests, and trees are considered while developing the IoV network communication [71–73]. In variable network density, as the IoV environment is quite huge, the density in the network of Internet of Vehicles varies. It depends on the traffic; in the case of a traffic jam, it can be high enough. Hence, frequent disconnection in the network is expected. Taking this into account, the variation in the network density shall be supported by the IoV communications so that the routing of data packets can be delivered correctly and in time. Either no or the minimum packet drop is expected [27, 31]. In highly dynamic topology, due to this, the topology of a vehicular network tends to change intermittently and with speed. Therefore, with the development of the IoV environment, the vast dynamics of the network topology must be carefully considered. IoV consists of several vehicles that frequently change their speed and direction. With that, the topology of the moving vehicles also changes [2, 17, 74]. Hence, IoV supports the highly dynamic topology, and the routing is based on considering the same.

7.2. Applications. The IoV supports several types of applications that are diverse. As the range of IoV is vast, the application the IoV communication supports is broader in range than the VANET [7, 38, 43, 75, 76]. Many researchers have proposed several areas of the IoV application. At a broader level, we can differentiate into three major categories, as shown in Figure 13.

7.2.1. Safety-Related Applications. Safety is the main feature when a driver is driving a car. To protect the driver and the passengers from any accidental or unwanted crashes, it is necessary to have safety-related applications in place [7]. The Collision Avoidance System is also known as CAS [8, 24]; it helps to pass on the information among the adjacent vehicles about the collision and informs the driver through beep sounds to avoid the collision; it uses V2V network communication to pass on the information as shown in Figure 14. CAS is also known as a precrash system which provides a collision warning for forwarding collision or the mitigation system of collision that uses the radar and the other sensors based on the laser or the camera to encountering the crash; after that, it produces a warning via alerting the driver on the cluster panel to apply the brakes well in time [4].

A fuzzy-based control algorithm is responsible for the safety of vehicle and the reliable distance to avoid the collision. Collision avoidance, lane-keeping assistance, adaptive cruise control, blind-spot detections, etc. are the few safety-related IoV applications. All the applications related to safety have time-bound constraints for the packets to be delivered. Otherwise, the result can be the collision of the vehicles.

7.2.2. Efficiency-Related Applications. The efficiency-related application or the vehicle's comfort-related application is also considered the essential requirements, and IoV plays a vital role in providing the necessary applications in the vehicles. Many applications are related to efficiency and comfort and generally divided into four significant ways: intersection control, route navigation, and parking navigation [8, 68].

In intersection control, the primary issue is to control the traffic at the intersections. The main point is to have efficient use of traffic signals to have less waiting time. Intersection traffic control can be traffic light-based or nontraffic light-based. The main problem in a traffic light system is to be aware of a signal strength scheduling plan. The traffic detectors are used to assemble the information on the traffic volume; thus, the traffic plan changes as per the difference in

Figure 14: Collision Avoidance System (CAS) in Internet of Vehicles (IoV).

the traffic conditions. Today's scenario is that by using V2V or V2I communication, the detailed vehicle information that includes the vehicle ID, speed, and the position is being collected, and according to that, the accurate and efficient scheduling is adopted. Similarly, there are techniques for intersection control that are based on nontraffic lights. In many algorithms, the driving behavior is controlled by the controller, which is called an intersection controller, that counts the ideal trajectory of each vehicle so that it can drive from the junction without collision [68].

In route navigation, navigation based on the vehicular network is to bypass the impediments of GPS-based navigations. Leontiadis et al. [77] suggested a system based on an ad hoc manner of crowd-sensing traffic information. This application helps to control environmental pollution via taking alternate routes and knowing before the traffic jams can save the consumption of petrol or diesel and save the environment from the pollution [20, 44, 71].

In parking navigation, to find available parking in urban areas is quite difficult, especially where shopping malls and offices are in the same place. It is a compelling issue. To solve the parking problem, IoV helps the driver know the parking space available to the driver well in time to provide efficiency [12, 78].

7.2.3. Infotainment-Related Applications. The applications related to infotainment mainly work on the internet services and the sharing of the files between the vehicles, as shown in Figure 15. Now, infotainment-related applications provide the notification and the alerts on the infotainment systems so that the driver can use all the features hands-free. It not only considers the entertainment aspect but also considers the alert that the infotainment-related applications have helped IoV take a new shape. With internet connectivity in a vehicle, there are several inbuilt applications for entertainment purposes that can be used by the driver and the passengers [24, 44]. Connecting the Android or iOS-based phones with the cable or via Wi-Fi provides an experience of entertainment and information function on the infotainment panel. Features like Siri and Google Assistant provide a hands-free experience for the driver to use phone operations with voice-based commands [5, 20, 41, 44]. Also, with the help of IoV communication, video sharing from one vehicle to another vehicle is possible.

7.3. Challenges in IoV. The goal of IoV is to adapt to different customers, heterogeneous networks, various vehicles, and many things and provide consistent connections that are always connected. The connection is expected to be convenient, manageable, maintainable, and safe as IoV is a complex system. In addition, IoV applications are different from other networks and need to consider many requirements. These aspects lead to various challenges in the IoV research and development, which have been mentioned as below [6, 79]: in lousy network connection and stability, due to the high flexibility and mobility of the vehicle and frequent topology changes resulting in repeated network failures and connection failures, loss of packets occurs. Hence, ensuring connectivity and coverage is still a challenge. Several routing protocols have been discussed in Section 5,

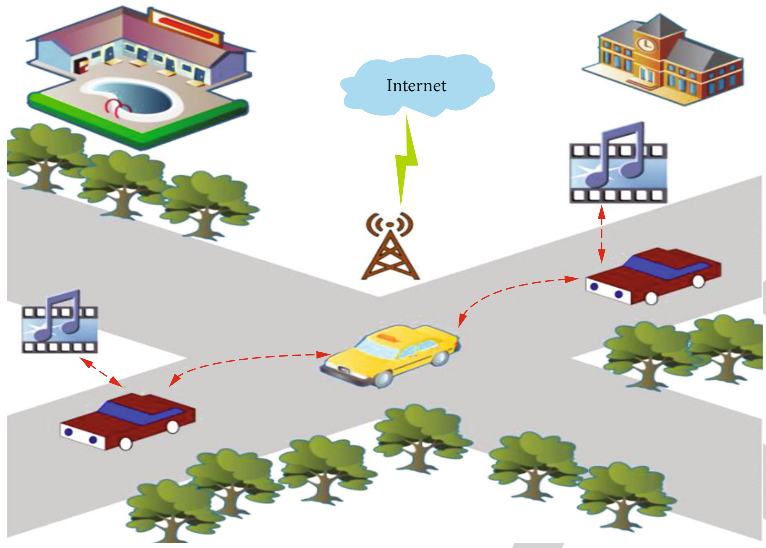

FIGURE 15: Videos sharing among vehicles in Internet of Vehicles (IoV).

and comparisons have been made. In a few routing protocols like VADD [80], PTCCR [59], ROAMER [54], and JBR [55], the delivery of packets ratio is good. However, with the very high increase in the speed of the vehicles, the OPBR [60] protocol results in an increase in the packet drop ratio, which is still a challenge in V2V communication.

In delay constraints, IoV applications have latency limitations but need not require high data rates. As an example, when an event of the brake occurs on the highway, then the trigger or the notification shall be made available in a proper amount of time to the other vehicles to avoid the crash. In this application, minimum delay rather than average delay is critical. There are several protocols like IGRTQ [67], OPBR [60], and VADD [80], which have the minimum E2E delay and outperform in packet delivery delay in comparison to other protocols like GPSR and GPCR. In high-reliability requirements, the applications based on driving are safety and sensitivity. For these types of applications, it is required to have very high reliability. Nevertheless, because of the network architecture and the network topography, achieving high reliability in IoV is difficult. The protocols, which are nondelay tolerant such as GPSR [57], Geographic Source Routing (GSR) [81], Greedy Perimeter Coordinator Routing (GPCR) [56], and Connectivity-Aware Routing protocol (CAR) [82], are considered suitable for the safety-related application; therefore, the nondelay tolerant characteristics may lead to the nonreliable behavior sometimes. However, the delay-tolerant protocols like VADD [80] and Reliable Routing Protocol proposed (RRP) [83] have good reliability and can be taken into consideration for infotainment or entertainment-related applications.

In service sustainability, it is quite a big challenge to persuade the sustainability of service in the IoV environment and the user-friendly design of the network mechanism for the IoV applications. Providing continuous services through heterogeneous networks in a real-time environment is a massive challenge because they are responsible for specific network bandwidth, limited-service platforms, different wireless access, and complex urban structures. [7, 44]. For the requirements for high scalability, it is a big challenge to handle the high scalability in IoV. As mentioned, IoV usually covers the number of the vehicle and the vast area. With such a large scale, it requires the Internet of Vehicles technology to have high scalability. Some protocols are suitable to consider for the high scalability requirements like GPCR [56] and medium scalability requirements like VADD [80] and IGRTQ [67]; however, there still exist protocols like RRP [83] which have very low scalability and cannot be considered for the dense or the high traffic conditions [2].

In security and privacy, the most challenging part of any IoV application is providing privacy and security to the users using the application. Therefore, authentication to the relevant user to provide trustworthy information from its starting point to the end is an utmost requirement. Ensuring that there is no breach of private information is still the critical challenge of IoV. IoV becomes vulnerable to cyberattacks. For example, if the hackers control the vehicle, they can easily manipulate the data or the different components like unlocking the vehicles without authentication, turning on/off the cars and failing the brakes, etc. Protocols like DSR [17, 74], in which request and response messages are associated, can be easily manipulated by hackers and cause potential danger. Similarly, in Ad hoc On-demand Distance Vector (AODV) [33], where straightforward communication mechanisms exist, attackers may advertise the smaller distance, and the routing table that can be updated can create a security threat in the protocol. Hence, authentication, integrity, access control, and nonrepudiation are the four basic security requirements that need consideration for IoV communication. Authentication [33, 71] provides the verification of the vehicle identification before transmitting any data packets to the vehicular network. Integrity [24, 71] ensures that any vehicle's data or transmitted by any vehicle must be validated correctly to ensure that data received and delivered is correct. Access control [2, 54] verifies that the vehicle accesses only those services to which they are entitled, and nonrepudiation [21, 41, 84] ensures the authentication so that the other vehicle shall not be denied its authenticity.

8. Conclusion

IoV is revamping the automotive system into a large and diverse car network, which has many benefits, including changes in information services, intelligent vehicle management, increased productivity, reduced traffic congestion, and car accidents. As a summary of this article, it provides an in-depth view of the various proposed architectures of IoV, and the seven-layer architecture is the most appropriate for IoV communication. The MAC and the network layer routing protocols have been discussed. The IEEE 802.11ac and 802.11ad are state-of-the-art MAC protocols used in IoV networks. OPBR and CBR are well suited for highway scenarios, while HNR, ACAR, and JBR are applicable in urban scenarios. The paper highlights various challenges in IoV such as security, scalability, bandwidth, and reliability concerning state-of-the-art and future enhancements that have been provided. The characteristics, along with the applications of IoV, have been described in detail. In conclusion, the IoV promotes automobiles and information technology, highlighting applications in terms of efficiency, safety, infotainment, connected devices, safety, and everything else. It eventually helps provide connectivity between vehicles, thereby improving the product and the services to the users.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this article.

Acknowledgments

This project was supported by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under grant No. KEP-11-611-42.

References

[1] P. Datta and B. Sharma, “A survey on IoT architectures, protocols, security and smart city based applications,” in *2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–5, Delhi, India, 2017.

[2] L. Tuyisenge, M. Ayaida, S. Tohme, and L. E. Afilal, *Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues*, vol. 11253, Springer International Publishing, 2018.

[3] I. Seth, S. N. Panda, and K. Guleria, “The essence of smart computing : Internet of Things,” in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, pp. 1–6, Noida, India, 2021.

[4] I. Seth, “A survey on driver behavior detection techniques,” *International Journal of Scientific & Technology Research*, vol. 7, no. 3, pp. 401–404, 2020.

[5] I. Seth, S. N. Panda, and K. Guleria, “IoT based smart applications and recent research trends,” in *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, 2021.

[6] N. Lu, N. Cheng, N. Zhang, X. Shen, and J. W. Mark, “Connected vehicles: solutions and challenges,” *IEEE Internet of Things Journal*, vol. 1, no. 4, pp. 289–299, 2014.

[7] W. Wu, Z. Yang, and K. Li, “Internet of Vehicles and applications,” in *Internet of Things: Principles and Paradigms*, pp. 299–317, Elsevier, 2016.

[8] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, “Vehicular ad hoc networks (VANETS): status, results, and challenges,” *Telecommunication Systems*, vol. 50, no. 4, pp. 217–241, 2012.

[9] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, “Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends,” *International Journal of Distributed Sensor Networks*, vol. 11, no. 8, 2015.

[10] R. S. Raw, D. K. Lobiyal, S. Das, and S. Kumar, “Analytical evaluation of directional-location aided routing protocol for VANETs,” *Wireless Personal Communications*, vol. 82, no. 3, pp. 1877–1891, 2015.

[11] T. K. Khattra and M. Mahajan, “ROUTING protocols for vehicular ad-hoc networks: a review,” *International Journal of Advanced Research in Computer Science*, vol. 5, no. 1, pp. 788–791, 2017.

[12] V. Verroios, V. Efstathiou, and A. Delis, “Reaching available public parking spaces in urban environments using ad hoc networking,” in *2011 IEEE 12th International Conference on Mobile Data Management*, vol. 1, pp. 141–151, Lulea, Sweden, 2011.

[13] N. Kumar, S. N. Panda, P. Pradhan, and R. Kaushal, “IoT based E-critical care unit for patients in-transit,” *Indian Journal of Public Health Research & Development*, vol. 10, no. 3, pp. 46–50, 2019.

[14] K. Guleria, A. K. Verma, N. Goyal, A. K. Sharma, A. Benslimane, and A. Singh, “An enhanced energy proficient clustering (EEPC) algorithm for relay selection in heterogeneous WSNs,” *Ad Hoc Networks*, vol. 116, article 102473, 2021.

[15] J. Zhang, F.-Y. Wang, K. Wang, W.-H. Lin, X. Xu, and C. Chen, “Data-driven intelligent transportation systems: a survey,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1624–1639, 2011.

[16] C. Manifesto, “CAR 2 CAR Communication Consortium Manifesto,” *System*, , IEEE Accessp. 94, 2007, https://ieeexplore.ieee.org/document/6799625.

[17] S. Singh and S. Agrawal, “VANET routing protocols: issues and challenges,” in *2014 Recent Advances in Engineering and Computational Sciences (RAECS)*, pp. 6–8, Chandigarh, India, 2014.

[18] P. Gandotra, R. Kumar Jha, and S. Jain, “A survey on device-to-device (D2D) communication: architecture and security issues,” *Journal of Network and Computer Applications*, vol. 78, pp. 9–29, 2017.

[19] M. A. Long, P. B. Stretesky, G. Harms, R. Sollund, and P. Macmillan, “Northumbria Research Link,” vol. 51, pp. 1–51, 2015, https://www.northumbria.ac.uk/nrl.

[20] O. Kaiwartya, A. H. Abdullah, Y. Cao et al., “Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects,” *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[21] J. G. Breslin, "Management with blockchain," in *5th International Conference, IOV 2018*, Paris, France, 2018.

[22] L. M. Ang, K. P. Seng, G. K. Ijemaru, and A. M. Zungeru, "Deployment of IoV for smart cities: applications, architecture, and challenges," *IEEE Access*, vol. 7, pp. 6473–6492, 2019.

[23] L. Alouache, N. Nguyen, M. Aliouat, and R. Chelouah, "Survey on IoV routing protocols: security and network architecture," *International Journal of Communication Systems*, vol. 32, no. 2, pp. 1–19, 2019.

[24] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibanez, "Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2018.

[25] I. Wahid, A. A. Ikram, M. Ahmad, S. Ali, and A. Ali, "State of the art routing protocols in VANETs: a review," *Procedia computer science*, vol. 130, pp. 689–694, 2018.

[26] A. Dua, N. Kumar, and S. Bawa, "A systematic review on routing protocols for vehicular ad hoc networks," *Vehicular Communications*, vol. 1, no. 1, pp. 33–52, 2014.

[27] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of Network and Computer Applications*, vol. 37, no. 1, pp. 380–392, 2014.

[28] P. K. Pandey, A. Swaroop, and V. Kansal, "A concise survey on recent routing protocols for vehicular ad hoc networks (VANETs)," in *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*, vol. 2019, pp. 188–193, Greater Noida, India, 2019.

[29] J. Cheng, J. Cheng, M. Zhou, F. Liu, S. Gao, and C. Liu, "Routing in internet of vehicles: a review," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 5, pp. 2339–2352, 2015.

[30] O. Senouci, Z. Aliouat, and S. Harous, "A review of routing protocols in internet of vehicles and their challenges," *Sensor Review*, vol. 39, no. 1, pp. 58–70, 2019.

[31] C. Ksouri, I. Jemili, M. Mosbah, and A. Belghith, "Towards general Internet of Vehicles networking: routing protocols survey," *Concurrency and Computation: Practice and Experience*, vol. 34, no. 7, article e5994, 2022.

[32] A. Tolba and A. Altameem, "A three-tier architecture for securing IOV communications using vehicular dependencies," *IEEE Access*, vol. 7, pp. 61331–61341, 2019.

[33] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, and Y. Park, "Authentication protocols in internet of vehicles: taxonomy, analysis, and challenges," *IEEE Access*, vol. 8, pp. 54314–54344, 2020.

[34] N. Liu, "Internet of vehicles: your next connection," *Huawei WinWin*, vol. 11, pp. 23–28, 2011.

[35] F. Bonomi, C. Fellow, and M. Others, *The Smart and Connected Vehicle and the Internet of Things*, CA: WSTS, San Jose', 2013.

[36] J. Wan, D. Zhang, S. Zhao, L. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions," *IEEE Communications Magazine*, vol. 52, no. 8, pp. 106–113, 2014.

[37] H. H. R. Sherazi, Z. A. Khan, R. Iqbal, S. Rizwan, M. A. Imran, and K. Awan, "A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication," *Mobile Information Systems*, vol. 2019, Article ID 3101276, 12 pages, 2019.

[38] A. Arooj, M. S. Farooq, T. Umer, G. Rasool, and B. Wang, "Cyber physical and social networks in IoV (CPSN-IoV): a multimodal architecture in edge-based networks for optimal route selection using 5G technologies," *IEEE Access*, vol. 8, pp. 33609–33630, 2020.

[39] H. Ji, O. Alfarraj, and A. Tolba, "Artificial intelligence-empowered edge of vehicles: architecture, enabling technologies, and applications," *IEEE Access*, vol. 8, pp. 61020–61034, 2020.

[40] H. Ji, O. Alfarraj, and A. Tolba, "Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[41] J. Contreras-Castillo, S. Zeadally, and J. A. G. Ibáñez, "A seven-layered model architecture for internet of vehicles," *Journal of Information and Telecommunication*, vol. 1, no. 1, pp. 4–22, 2017.

[42] K. Collins and G. M. Muntean, "Route-based vehicular traffic management for wireless access in vehicular environments," in *2008 IEEE 68th Vehicular Technology Conference*, pp. 3–7, Calgary, AB, Canada, 2008.

[43] S. Yu, J. Lee, K. Park, A. K. Das, and Y. Park, "IoV-SMAP: secure and efficient message authentication protocol for IoV in smart city environment," *IEEE Access*, vol. 8, pp. 167875–167886, 2020.

[44] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China communications*, vol. 11, no. 10, pp. 1–15, 2014.

[45] I. Seth, K. Guleria, and S. N. Panda, "Introducing intelligence in vehicular ad hoc networks using machine learning algorithms," *ECS Transactions*, vol. 107, no. 1, 2022.

[46] Q. Xu, H. Fan, S. Guo, and X. Xiao, "A context-aware MAC protocol for VANETs," in *International Conference on Wireless Algorithms, Systems, and Applications*, vol. 7992, pp. 135–150, Berlin, Heidelberg, 2013.

[47] A. N. Dharsandiya and R. M. Patel, "A review on MAC protocols of vehicular ad hoc networks," in *2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, pp. 1040–1045, Chennai, India, 2016.

[48] S. A. Gillani, P. A. Shah, A. Qayyum, and H. B. Hasbullah, "MAC layer challenges and proposed protocols for vehicular ad-hoc networks," *Advances in Intelligent Systems and Computing*, vol. 306, no. July, pp. 3–13, 2015.

[49] M. Ma, K. Liu, X. Luo, T. Zhang, and F. Liu, "Review of mac protocols for vehicular ad hoc networks," *Sensors (Switzerland)*, vol. 20, no. 23, pp. 1–28, 2020.

[50] A. Sharma, N. Goyal, and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes," *The Journal of Supercomputing*, vol. 77, no. 6, pp. 6036–6055, 2021.

[51] K. Guleria and A. K. Verma, "Comprehensive review for energy efficient hierarchical routing protocols on wireless sensor networks," *Wireless Networks*, vol. 25, no. 3, pp. 1159–1183, 2019.

[52] Q. Yang, A. Lim, S. Li, J. Fang, and P. Agrawal, "ACAR: adaptive connectivity aware routing for vehicular ad hoc networks in city scenarios," *Mobile Networks and Applications*, vol. 15, no. 1, pp. 36–60, 2010.

[53] Y. Luo, W. Zhang, and Y. Hu, "A new cluster based routing protocol for VANET," in *2010 Second International Conference on Networks Security, Wireless Communications and Trusted Computing*, vol. 1, pp. 176–180, Wuhan, China, 2010.

[54] K. Mershad, H. Artail, and M. Gerla, "ROAMER: roadside units as message routers in VANETs," *Ad Hoc Networks*, vol. 10, no. 3, pp. 479–496, 2012.

[55] S. Tsiachris, G. Koltsidas, and F. N. Pavlidou, "Junction-based geographic routing algorithm for vehicular ad hoc networks," *Wireless Personal Communications*, vol. 71, no. 2, pp. 955–973, 2013.

[56] A. Bazzi and A. Zanella, "Position based routing in crowd sensing vehicular networks," *Ad Hoc Networks*, vol. 36, pp. 409–424, 2016.

[57] B. Karp and H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, pp. 243–254, Boston, Massachusetts, USA, 2000.

[58] O. Alzamzami and I. Mahgoub, "Fuzzy logic-based geographic routing for urban vehicular networks using link quality and achievable throughput estimations," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 6, pp. 2289–2300, 2019.

[59] C. Chen, T. Xiao, M. Zhang, and Q. Pei, "PTCCR: a path transmission costs-based multi-lane connectivity routing protocol for urban internet of vehicles," *IEEE Access*, vol. 7, pp. 141838–141849, 2019.

[60] A. Ghaffari, "Hybrid opportunistic and position-based routing protocol in vehicular ad hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 4, pp. 1593–1603, 2020.

[61] H. Gao, C. Liu, Y. Li, and X. Yang, "V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3533–3546, 2021.

[62] K. Mershad, "SURFER: a secure SDN-based routing protocol for Internet of Vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7407–7422, 2020.

[63] R. Attia, A. Hassaan, and R. Rizk, "Advanced greedy hybrid bio-inspired routing protocol to improve IoV," *IEEE Access*, vol. 9, pp. 131260–131272, 2021.

[64] S. Sennan, S. Ramasubbareddy, S. Balasubramaniyam, A. Nayyar, C. A. Kerrache, and M. Bilal, "MADCR: mobility aware dynamic clustering-based routing protocol in Internet of Vehicles," *China Communications*, vol. 18, no. 7, pp. 69–85, 2021.

[65] A. Hawbani, X. Wang, A. al-Dubai et al., "A novel heuristic data routing for urban vehicularad hocnetworks," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 8976–8989, 2021.

[66] C. Chen, L. Liu, T. Qiu, J. Jiang, Q. Pei, and H. Song, "Routing with traffic awareness and link preference in Internet of Vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 200–214, 2022.

[67] L. Liu, C. Chen, Z. Ren, and F. R. Yu, "An intersection-based geographic routing with transmission quality guaranteed in urban VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 1, pp. 200–214, 2022.

[68] U. Z. A. Hamid, H. Zamzuri, and D. K. Limbu, "Internet of vehicle (iov) applications in expediting the implementation of smart highway of autonomous vehicle: a survey," *Performability in Internet of Things*, vol. 2018, pp. 137–157, 2019.

[69] N. Li, J. F. Martinez-Ortega, V. H. Diaz, and J. A. S. Fernandez, "Probability prediction-based reliable and efficient opportunistic routing algorithm for VANETs," *IEEE/ACM Transactions on Networking*, vol. 26, no. 4, pp. 1933–1947, 2018.

[70] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for Vehicular Ad hoc NETworks (VANETs): a survey," *Vehicular Communications*, vol. 11, pp. 20–31, 2018.

[71] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, "IEEE transactions on computers VSPN : VANET-based Secure and Privacy-preserving Navigation," *IEEE Transactions on Computers*, vol. 63, no. 2, pp. 510–524, 2012.

[72] D. Lin, J. Kang, A. Squicciarini, Y. Wu, S. Gurung, and O. Tonguz, "MoZo: a moving zone based routing protocol using pure V2V communication in VANETs," *IEEE Transactions on Mobile Computing*, vol. 16, no. 5, pp. 1357–1370, 2017.

[73] Y. Li, A. Mohaisen, and Z. L. Zhang, "Trading optimality for scalability in large-scale opportunistic routing," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 5, pp. 2253–2263, 2013.

[74] D. Tian, C. Zhang, X. Duan, Y. Wang, J. Zhou, and Z. Sheng, "A multi-hop routing protocol for video transmission in IoVs based on cellular attractor selection," *Future Generation Computer Systems*, vol. 95, pp. 713–726, 2019.

[75] S. Keshari, V. Kansal, and S. Kumar, "A cluster based intelligent method to manage load of controllers in SDN-IoT networks for smart cities," *Scalable Computing: Practice and Experience*, vol. 22, no. 2, 2021.

[76] S. K. Keshari, V. Kansal, and S. Kumar, "A systematic review of quality of services (QoS) in software defined networking (SDN)," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2593–2614, 2021.

[77] I. Leontiadis, G. Marfia, D. Mack, G. Pau, C. Mascolo, and M. Gerla, "On the effectiveness of an opportunistic traffic management system for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 4, pp. 1537–1548, 2011.

[78] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: a new VANET-based smart parking scheme for large parking lots," in *IEEE INFOCOM 2009*, pp. 1413–1421, Rio de Janeiro, Brazil, 2009.

[79] E. Khoza, C. Tu, and P. A. Owolawi, "Comparative study on routing protocols for Vehicular Ad-Hoc Networks (VANETs)," in *2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, pp. 1–6, Durban, South Africa, 2018.

[80] J. Zhao and G. Cao, "VADD: vehicle-assisted data delivery in Vehicular *Ad Hoc* Networks," *IEEE Transactions on Vehicular Technology*, vol. 57, no. 3, pp. 1910–1922, 2008.

[81] T. Nebbou and M. Lehsaini, "Greedy curvemetric-based routing protocol for VANETs," in *2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT)*, pp. 1–6, Tangier, Morocco, 2018.

[82] K. Shafiee and V. C. M. Leung, "Connectivity-aware minimum-delay geographic routing with vehicle tracking in VANETs," *Ad Hoc Networks*, vol. 9, no. 2, pp. 131–141, 2011.

[83] A. I. Saleh, S. A. Gamel, and K. M. Abo-Al-Ez, "A reliable routing protocol for vehicular ad hoc networks," *Computers and Electrical Engineering*, vol. 64, pp. 473–495, 2017.

[84] G. D. Singh, R. Tomar, H. G. Sastry, and M. Prateek, "A review on VANET routing protocols and wireless standards," *Smart Innovation, Systems and Technologies*, vol. 78, pp. 329–340, 2018.