Survey of Interoperability Challenges in the Internet of Vehicles

Paul Agbaje[1], Afia Anjum[1], Arkajyoti Mitra[1], Emmanuel Oseghale[1], Gedare Bloom[2] *Senior Member, IEEE*,
Habeeb Olufowobi[1] *Member, IEEE*
1: *University of Texas at Arlington*, Arlington, TX, USA
2: *University of Colorado Colorado Springs*, Colorado Springs, CO, USA
Email: {pauloluwatowoju.agbaje, afia.anjum, arkajyoti.mitra, emmanuelemakhue.oseghale, habeeb.olufowobi}@uta.edu,
gbloom@uccs.edu

***Abstract*—The Internet of Vehicles (IoV) is an active area for innovation and an essential tool in achieving smart cities through the integration of vehicles with the Internet of Things (IoT). IoV is a distributed network that aids in handling the data generated by vehicular sensors and vehicle-to-everything communication (V2X), thus enabling novel applications such as autonomous driving and platooning while increasing safety and energy efficiency. In IoV, the sensors and the interdependent devices relay critical information for the efficient implementation of real-time applications in the ecosystem. Despite all these advancements, a vital challenge is establishing smooth communication among interconnected devices, concretely, interoperability in the IoV—a deceptively simple notion that is not yet fully addressed to achieve a fully integrated ecosystem. This is mainly because the networked domains, such as home, grid, and health care, are developed in silos, operating independently with diverse processes and protocols. Hence, seamless exchange of information is yet to be achieved across the ecosystem, hindering the maximization of the full promise of IoV. In this paper, we provide an in-depth analysis of the present state of interoperability and comprehensively survey the challenges in IoV. We present a taxonomy of interoperability approaches, review solutions that prior work have proposed, and provide insights on how to address the current challenges. Finally, we identify open problems that persist and future directions for research.**

***Index Terms*—Internet of Vehicles, Interoperability, Smart City, Intelligent Transportation System**

I. Introduction

The increasing proliferation of communication technologies in vehicles, the surrounding infrastructure, and their connectivity to the Internet conceptualizes the idea of a “vehicle” as another “Thing”, bringing about the concept of the Internet of Vehicles (IoV) as an extension of the Internet of Things (IoT). IoV connects hardware devices, network communication channels, and cloud platforms [1] that allow connected vehicles, pedestrians, and intelligent units near the road to exchange information in real-time. This information is used to make transportation and vehicle maintenance processes more cost-effective, provide situational awareness, safety and comfort, transportation efficiency, and address growing urbanization challenges. The IoV is a highly integrated application of the IoT and intelligent transportation systems (ITS) that originated from vehicular ad hoc networks (VANETs), enabling automobiles to form spontaneous wireless connections [2]. In IoV, intelligent and connected vehicles need a reliable connection and communication to the underlying infrastructure, other vehicles, and nearby humans. This communication produces varied and vast data stored in the cloud for ease of access and analytics, which enables a smart city ecosystem [3].

The benefits of a fully connected IoV ecosystem drive the need to achieve the full inter-working of all the entities in it. As defined by IEEE in its glossary of software engineering terminology, interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged [4]. This definition implies that entities in the IoV should be able to share and transfer data reliably. Furthermore, the data shared among these entities must be usable to support IoV applications and services. However, the diversity and complexity of applications and end nodes with different data formats and internal architecture make the seamless integration of components in the IoV a challenge [5]. IoV is a large-scale, decentralized network with inherent heterogeneous connections of cyber and physical components operating in highly dynamic environments.

Prior work investigate problems that relate to vehicles’ communication to everything (V2X). As shown in Figure 1, V2X consists of vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-roadside units (V2R), vehicle-to-pedestrian (V2P), vehicle-to-grid (V2G), vehicle-to-building (V2B), vehicle-to-device (V2D), and vehicle-to-cloud (V2C) communications. Overcoming the challenges of integrating these heterogeneous entities will enable the efficient implementation of IoV applications. In addition to the heterogeneity, vehicular networks are characterized by their dynamic nature. This dynamism affects the delivery of data in the network, which makes reliable communications difficult [6]. Also, with the advancement in communication networks and artificial intelligence (AI), the capabilities of traffic management systems will continue to improve. This advancement implies that connected entities in IoV need to meet different quality of service (QoS) requirements for real-time traffic monitoring, low latency communication, and minimal dropped packets.

The interplay between IoV entities presents a paradoxical communication framework that does not guarantee seamless interactions and information sharing in real-time. IoV is enabled by application domains with multiple requirements and information models to offer services to users, such as collision avoidance system and emergency services. The ve-

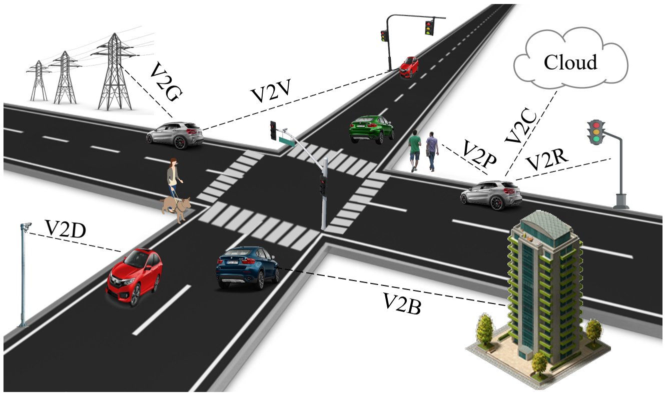


Fig. 1: IoV Ecosystem

hicles in IoV function in an IoT environment that contains a myriad of devices with diverse technical profiles operating with different standards. Here, application interactions and information sharing should be seamless across the network to coordinate vehicular movement and the safety of road users. This interaction requires the mutual consensus of the entities in the IoV ecosystem, which is presently a technical challenge. Currently, the device market is fragmented, and these entities have different communication protocols and standards that hinder the exchange of information critical to realizing a fully integrated ecosystem that supports real-time applications.

We make the following contributions in this paper:

- We comprehensively describe the IoV ecosystem and entities in it which are pertinent to the realization of seamless integration for interoperability.
- We present the criteria for interoperability in IoV based on prior surveyed work and provide analyses of possible future directions.
- We propose five distinct categories of interoperability challenges in IoV that stand in the way of realizing the promises of an harmonious IoV ecosystem.
- We summarize interoperability solutions in the literature and the associated challenges that remain related to their implementation.
- We discuss open problems and identify future research challenges that still need to be addressed in IoV interoperability.

The remainder of the paper is organized as follows. We review related work in Section II and present an overview of the IoV ecosystem in Section III. In Section IV, we provide a taxonomy of IoV interoperability and present approaches that have been used to solve IoV interoperability challenges in Section V. In Section VI we provide some open research problem that need to be addressed to solve pending interoperability issues in IoV. Section VII concludes the work.

II. Related Work

In this section, we first review the related work on interoperability specific to different platforms, the IoT domain [7]–[10], and IoT application-specific approaches [11]–[15] before discussing the work on IoV interoperability [5], [16], [17].

Application and platform specific interoperability solutions were explored in different work [11]–[15]. To solve interoperability concerns in the smart home environment, Perumal et al. [11] present a solution based on simple object access protocol technology (SOAP), Moon et al. [12] recommend the construction of a program called universal middleware bridge, and Park et al. [13] present a system called multimedia room bridge adapter. Using a framework based on virtual overlay networks, Park et al. [14] address interoperability concerns in the ubiquitous home, which comprises both home and out-of-home devices. Zeid et al. [15] focus on interoperability challenges in the context of smart manufacturing. The authors explore syntactic, semantic, factory, and cloud manufacturing interoperability, as well as architectural model solutions given by well-known platforms, such as Industries 4.0 and Industrial Internet Consortium (IIC). Pantsar-Syväniemi et al. [18] presented an adaptation framework for situation-based and self-adaptive applications in smart environment consisting of five layers of interoperability: connection (network connectivity), communication (syntax of data), semantic (understanding data), dynamic (context changes), behavioral (matching actions), and conceptual (modeling and abstraction). However, the work described above are specifically for smart home, smart manufacturing, and smart environment and are unlikely to generalize to the IoV.

Noura et al. [7] present a survey of challenges of interconnecting heterogeneous devices, and the techniques to address them in the diverse platforms of the IoT. These techniques include using tools provided by adapters/gateways, such as mediators, creating virtual networks on top of the physical layer, networking technologies, open application programming interfaces (APIs), and service oriented architectures built on top of the network layer. Lee et al. [8] posit that to achieve interoperability and security in the IoT, compatibility, generality, and international standards that are defined and approved by authorized organizations must be considered. Hence, the authors study and summarize the international standards related to interoperability and security for IoT. Rahman et al. [9] survey approaches to address semantic interoperability of IoT by classifying them into ontology, middleware, and the semantic web. Also, frameworks and tools used for validating and evaluating the interoperability of IoT are discussed while pointing out open research issues that need to be addressed. Konduru and Bharamagoudray [10] detail probable challenges of addressing IoT interoperability suggesting that lack of resources, using proprietary technology, the complexity of the network, disparate security requirements, and heterogeneous devices make it difficult to interwork all the entities of the IoT ecosystem. The authors also identify some already developed open source tools, frameworks, and APIs, such as Google Weave, IoTivity, Alljoyn, and Apple Home Kit, that aim to address the issues of IoT interoperability. However, inter-device communication in IoV presents domain-specific challenges, such as complex data syntax, mobility, and dynamic network topologies, that make proposed IoT solutions insufficient to address interoperability challenges IoV.

Prior work on IoV interoperability challenges and solutions further refine IoT interoperability to the transportation infrastructure domain. Hussain et al. [16] present syntactic, semantic, and cross-domain interoperability. The authors identify the

TABLE I: List of acronyms

Acronym	Full meaning	Acronym	Full meaning	Acronym	Full meaning
A-GW	Access Gateway	MR	Mobile Router	VANET	Vehicular ad hoc Networks
AI	Artificial Intelligence	NDN	Named Data Networking	VDTN	Vehicular Delay Tolerant Networks
API	Application Programming Interface	NEMO	Network Mobility	VNDN	Vehicular Named Data Networking
BS	Base Station	OWL	Web Ontology Language	VSDN	Vehicular Software Defined Networking
C-V2X	Cellular Vehicle-to-Everything	PHY	Physical Layer	V2B	Vehicle-to-Building
DSRC	Dedicated Short-range Communications	QoS	Quality of Service	V2C	Vehicle-to-Cloud
DTN	Delay Tolerant Networks	RL	Reinforcement Learning	V2D	Vehicle-to-Device
EV	Electric Vehicles	RSU	Road-side Unit	V2G	Vehicle-to-Grid
FMA	Foreign Mobile agent	SDN	Software Defined Networking	V2H	Vehicle-to-Home
HA	Home agent	SEAD	Simple Efficient Adaptive Data Protocol	V2I	Vehicle-to-Infrastructure
IIC	Internet Consortium	SIoV	Social Internet of Vehicles	V2P	Vehicle-to-Pedestrian
IoT	Internet of Things	SL-ZRP	Stable Link Zone Routing Protocol	V2R	Vehicle-to-Roadside Units
IoV	Internet of Vehicles	SOAP	Simple Object Access Protocol	V2V	Vehicle-to-Vehicle
ITS	Intelligent Transportation Systems	SRP	Stream Reservation Protocol	V2X	Vehicle-to-Everything
IVC	Inter Vehicular Communication	TCP	Transmission Control Protocol	WAVE	Wireless Access in Vehicular Environment
LTE	Long Term Evolution	ToD	Trend of Delivery	WiMAX	Worldwide Interoperability for Microwave Access
LTE-A	Long Term Evolution Advanced	UAV	Unmanned Aerial Vehicle	XML	Extensible Markup Language
MAC	Medium access control	UBI	User Based Insurance		

pros and cons of interoperability strategies including increased execution time, latency, and a lack of mobility support. Hussain et al. [17] explore the factors that make interoperability challenging by highlighting the lack of standards that could enable seamless interconnection of IoV components. They propose a seven-layer taxonomy of interoperability in IoV that include no interoperability, technical, syntactic, semantic, pragmatic, dynamic, and conceptual interoperability. They also suggest that using IoT middleware solutions can help in achieving interoperability in IoV. However, the authors did not provide the details of the middleware solution and how it can address interoperability in the IoV. Datta et al. [5] describe vehicles as connected resources that deliver services, such as traffic management and pollution detection, for smart cities. The authors identify that a lack of uniform architecture and standards, and the presence of data silos, prevented the development of a fully connected IoV that integrates customers, automobiles, and computing platforms. To address these concerns, they propose an IoT architecture that utilizes open standards, such as SenML, oneM2M, and semantic web technologies, for interoperability in the IoV. Moreover, they outlined the operational phases of the proposed framework and how it can be used as a reference for developing IoV applications.

However, the proposed IoV solutions did not address the dynamic topology and the heterogeneity of devices and data communicated in the IoV ecosystem. Our work differs from previous work by focusing on unifying the assumptions, challenges, strategies implemented, and research problems existing in the research area of IoV interoperability. We provide a comprehensive taxonomy of interoperability in IoV considering the heterogeneity and dynamic topology of vehicular networks and present a detailed analysis of the requirements of interworking heterogeneous entities in the IoV. We also present a study of open problems to establish a seamless, integrated IoV ecosystem.

III. Overview of IoV Ecosystem

In this section, we give a background of the IoV ecosystem and its communicating nodes. We also describe the IoV framework, its applications, and the users in the ecosystem. Figure 2 highlights the three layer architecture mapping of the IoV framework, and Figure 3 further refines the layered framework to organize the IoV ecosystem.

A. IoV Framework

IoV enables vehicles to communicate with other entities in its operating environment by providing a platform that integrates “things”, intelligent cars, humans, and the surrounding infrastructure through networking channels and the Internet. IoV allows vehicles to interact with each other (V2V), as well as communicate with intelligent devices (V2D), grid (V2G), buildings (V2B), roadside units (V2R), and the cloud (V2C) to create heterogeneous and highly connected systems supporting diverse applications and functions. This interaction allows the entities of the ecosystem to exchange information and work together to create an intelligent system that supports services for smart cities [19]. IoV is envisioned to enhance road safety through autonomous driving and platooning, mitigate traffic congestion, decrease pollution, and facilitate ride-sharing services for space and cost-saving [20]. IoV is primarily different from ITS as it transforms every vehicle into an intelligent node on the highway, with its own compute, storage, and networking capability for information sharing among vehicles, humans, and the surrounding road infrastructure.

Based on the interplay of communicating nodes, there have been several proposed architectural layers for IoV [3], [21], [22]. The architecture comprises perception, network, and application layers, described below. Each layer requires multi-level cooperation to enable connectivity and interoperability. IoV has several immaculate data sources (heterogeneous devices) at the perception layer and software and applications to analyze sensed and collected device data at the application layer. However, the network layer is critical to the IoV operations as it enables connectivity, data extraction, transmission, and security between the other two layers. The network layer is

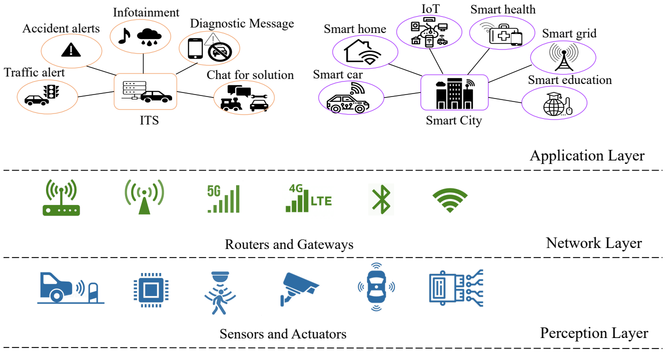


Fig. 2: IoV Layered Architecture [21]

uniquely positioned at the center of the framework to support the functional requirements and manageability of devices and the layers, bringing about efficient V2X communication.

1) Perception Layer: The perception layer is at the lowest level hosting the edge devices, including the sensors, actuator, and the associated computational capabilities. This layer achieves data sensing and collection using the sensors embedded in the vehicles that enable capturing information about the physical environment, including road and traffic conditions, objects, and driving behaviors. The data gathered by the perception layer are usually extensive, covering a wide range of sensor information that requires cooperation between different IoV entities for efficient optimization of available resources [23]. In addition, analog data gathered in the layer are converted into digital formats for further processing, storage, and distribution [24]. The edge devices process the collected data locally, often in real-time, and communicate information with other devices in the layer or the network through wireless and wired connections. Technologies used in this layer for wireless connection include WiFi, Bluetooth, ZigBee, and radio-frequency, while traditional serial connections, such as I2C, SPI, and Ethernet, are used for wired connectivity [25].

Since the devices in the perception layer use different technologies and protocols to relay information, achieving interoperability is crucial to ensure that these devices can send sensed data efficiently across the network. Interoperability in the perception layer should ensure that sensors and other devices in the IoV can continuously communicate and dynamically join the vehicular network. In addition, the adoption of standards would ensure that devices are manageable and connected irrespective of their underlying technology, specifications, or models [26].

2) Network Layer: This layer enables the communication between nodes in IoV by using network technologies for determining the routes for sensor data to various services. This layer uses devices like gateways, switches, hubs, and routing devices to facilitate information communication. Some of the technologies used include wireless access in vehicular environment (WAVE), worldwide interoperability for microwave access (WiMAX), 4G/LTE, 5G/6G, Bluetooth, and WiFi to transmit data to applications in heterogeneous networks. Each of these technologies has its strengths and weaknesses. For example, WAVE provides connectivity for devices using dedicated short-range communications (DSRC), supporting vehicles moving with a speed of up to 200km/h [27]. However, an increase in the vehicle speed can lead to an increasing number of dropped packets across the network [28]. Moreover, 4G and LTE may also fail to meet the QoS requirements of dense networks that process large packet frames.

Exploiting the advantages of these technologies for communication among devices in the ecosystem requires overcoming integration challenges as they have diverse connection interfaces and protocols. The network layer needs to be robust, reliable, and stable to accommodate different requirements and ensure optimal resource utilization by every application as it brings everything together. In addition, the network layer should support mobility management, efficient hand-off, and robust network traffic management techniques that would guarantee the network QoS.

3) Application Layer: The application layer is the topmost layer that provides support for data processing, storage, and analysis. This layer facilitates the interaction of user and user application and uses the data provided by the perception layer to provide services for ITS (e.g., infotainment, traffic management, remote diagnostics) and smart cities. Furthermore, this layer defines protocols needed for data transmission across the network and interfaces that allow interactivity among applications in the ecosystem.

Applications should be able to interact across heterogeneous platforms, share resources, and communicate efficiently with other applications and network services. In addition, applications should include easy-to-use user interfaces that enhance interaction. Achieving interoperability among applications across different platforms in IoV is critical to ensuring that users can efficiently use available services and resources. Provided below is a detailed discussion of existing IoV applications.

B. IoV Applications

IoV applications can be broadly classified into two: (1) applications for ITS, and (2) applications for smart cities [29]. In this section we discuss each of these applications relating to IoV, and their classifications.

1) Applications for Intelligent Transportation Systems: ITS are a broad spectrum of technologies applied to make the transportation system more reliable, more efficient, safer, and at the same time environmentally friendly without necessarily having to alter current infrastructure [30]. The applications of IoV relating to ITS can be grouped into five major categories:

1) *Safety:* IoV applications that are concerned with safety help improve the chances of avoiding accidents by vehicles. Generally, safety applications for vehicles are called collision avoidance systems [29]. Prior work investigate safety-based IoV applications like forward collision warning system [31], vehicle detection using active learning and symmetry [32], and other approaches based on machine learning [33], [34] or night vision [35]. To protect road users, the seamless integration of safety-critical applications in the IoV ecosystem is not negotiable. Vehicles must be able to communicate both internally and externally with other vehicles and road

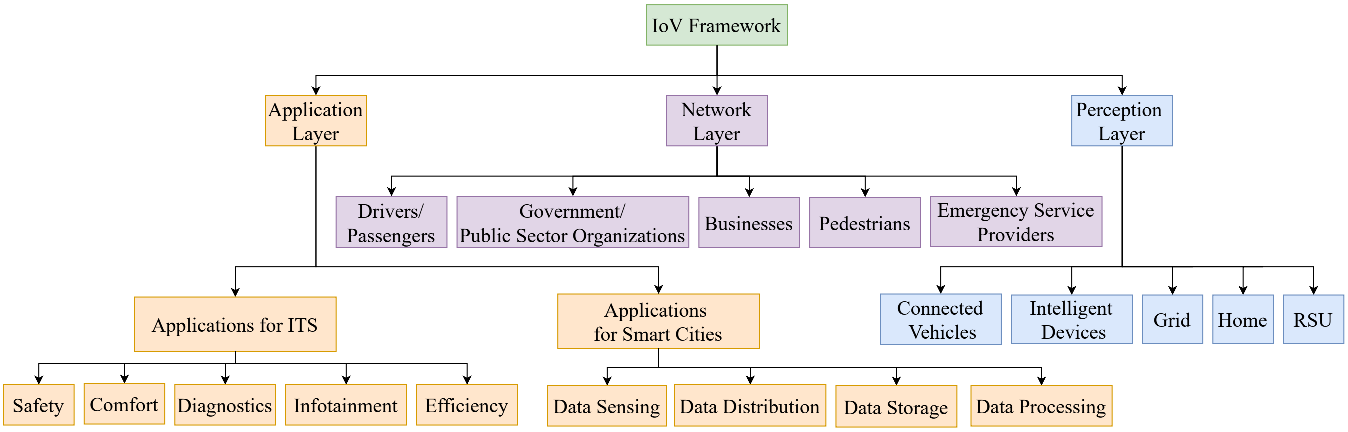


Fig. 3: Hierarchical decomposition of IoV architectural layers

users, notifying them of potential and present collisions to ensure safety.

2) *Comfort:* Applications based on comfort aim to improve the convenience of passengers and drivers. Users now require a degree of modularity and configurability within vehicle interior and human-machine interface to interact with in-vehicle functions more conveniently via speech recognition. Connections between devices must be efficient to make these communications work seamlessly. The heterogeneous nodes need to be able to communicate over an integrated protocol, and the applications involved need to be able to send data in formats that can be interpreted and processed by the receiving nodes.
3) *Diagnostics:* Correct and efficient diagnosis is crucial for vehicular operation. Vehicular diagnostics information is essential to troubleshoot faults that may arise in any part of a vehicle's system. Users can receive fault information on other intelligent devices like their mobile phones and the in-vehicle display units. For remote diagnostics to be effectively carried out, end-nodes must be seamlessly connected, and diagnostics applications must be fully integrated into the ecosystem. Channels of communication must be reliable for the efficient operation of real-time monitoring and diagnostics.
4) *Infotainment:* Infotainment applications provide both information and entertainment updates to vehicle users. A degree of connectivity to enable work or onboard entertainment that could improve the traveling experience of the occupants of a vehicle is desirable. Applications that allow these services are imperative, and with the seamless interworking of IoV entities, streaming media services can provide personalized and location-based content to vehicle occupants while traveling.
5) *Efficiency:* Applications based on efficiency in IoV aim to improve eco-friendly driving and traffic management within the ecosystem. Eco-friendly driving practices, such as efficient braking at intersections and management of acceleration, facilitate the optimization of energy usage [36]. Furthermore, efficient management of traffic is essential in smart cities to achieve safe and organized road usage. Solutions that solve existing interoperability challenges in IoV are required to support these applications and provide efficient management of IoV resources, which has not been adequately explored.
6) *Security:* Prevalent in the autonomous vehicle domain are availability and integrity attacks, such as denial of service, spoofing, and Sybil attacks that negatively impact the QoS of entities and safety applications in the IoVs. Applications for IoV security ensure that communications are reliable and secure by satisfying the requirements for confidentiality, authenticity, availability, integrity, and non-repudiation [37]. For the efficient implementation of security in IoV, standards such as WAVE and European Telecommunications Standards Institute describe the security profiles, data structures, and certificate formats necessary for secure ITS communication [38]. Also, solutions that address security issues in IoVs have included the use of encryption, digital signatures, and intrusion detection and prevention systems to enforce confidentiality, authentication, and data integrity in traffic data and disaster recovery within the ecosystem [39].
7) *Privacy:* With the vast number of sensors in the IoV, there is a considerable amount of data shared between end nodes, edge devices, and the cloud for processing, analytics, and storage. A vital aspect of maintaining the privacy of IoV users is protecting these data from unintended access and use. Privacy issues include the misuse of location and trajectory data of vehicles, users' images and electronic credentials, and privately collected data by cloud and edge servers. In IoV, efficient privacy-enforcement frameworks and schemes are essential to ensure a reliable ecosystem free from privacy infringements and data misuse [37].

2) Applications For Smart Cities: The ability of nodes to rapidly exchange data makes IoV a valuable resource for smart cities. IoV can be utilized to meet the needs of smart cities for large-scale intelligence data gathering, transfer, and processing from the embedded sensors in the smart city environment. Also, as data on wheels, the vehicles in IoV have fewer constraints related to battery life or information processing capabilities compared to traditional wireless sensor networks [29]. Each communicating object of IoV is perceived to perform four roles [29]:

- *Peers:* In IoV, each node is connected with other nodes to maintain a network for sharing resources. The vehicle entities acting as peers help establish and maintain network connectivity in the IoV.
- *Clients:* The vehicle objects acting as clients initiate requests and consume services from IoV.
- *Data Collectors (Mules):* These collect data generated by intelligent nodes and transmit the data to servers for further processing.
- *Distributed Computing Resources:* Since individual smart object in IoV have constrained compute, memory, and power resources, the communicating nodes use a distributed computing paradigm, enabling the individual nodes to work together and increase the computational power available to nodes.

With all these roles, IoV is vital to smart cities by achieving data sensing, data collection, data processing and data distribution capabilities, which are discussed below.

1) *Data Sensing:* Nodes in IoV, such as vehicles, have embedded sensors that absorb information from the environment to support traffic condition monitoring and management, navigation, and detecting changes. The amassed data can be used in smart city applications, e.g., air pollution control and service personalization.
2) *Data Collection:* Vehicles and other nodes in IoV can assist in gathering data from different geographical locations in smart cities. In addition, they can assist in the aggregation of data from various sources for further processing and distribution [40].
3) *Data Processing:* The ability of vehicular nodes to be used as distributed computing resources enable their usage as edge computing devices. In addition, mobile vehicles can be organized to form vehicular clouds to offer real-time computational capacity for smart city applications [41].
4) *Data Distribution:* Smart city nodes trying to send information to other nodes can use vehicles as relays to support caching and forwarding. In addition, vehicular nodes can assist in delivering critical environmental information during emergencies. [42].

C. IoV Nodes

The nodes in the IoV provide resources for applications and services, and benefit from such services. These nodes include connected vehicles, intelligent devices, grid, homes, road side units (RSUs), and the cloud.

1) Connected Vehicles: Vehicles are mobile nodes that support communication with other vehicles on the road. With the availability of V2V technologies and DSRC, the collaboration of vehicles can help to improve safety and ensure cooperative ITS. The basic message sent from vehicles can also be used for safety, weather, and mobility applications [43]. Apart from data transfer capability, vehicles are a valuable resource for sensing, monitoring, and processing collected data. Also, the cars and trucks can serve as edge computing devices whereby resources are pulled together for use as distributed computing platforms.

2) Intelligent Devices: V2D communication allows electronic devices to connect with vehicles for information exchange through protocols such as Bluetooth, WiFi, and LTE-Direct without relying on traditional communications infrastructure, e.g., base stations (BSs). Intelligent road signs and traffic lights are some devices that can communicate with cars for efficient traffic management. These technologies permeate the smartphone market with enabling applications like Apple's CarPlay, Mirror links, and AndroidAuto, allowing mobile phones, tablets, and wearables to transfer their display and communicate with the vehicle's built-in infotainment display. These technologies provide added comfort and allow users to manage vehicular resources more efficiently. A computer can also remotely connect to vehicles to retrieve diagnostics information and to monitor the condition of vehicles on the road. Another area of usage of these devices is in computer vision applications that allow videos collected from cameras to be sent for preprocessing and then used in traffic management systems [44]. These devices require full integration to reduce latency to minimize the risks of traffic gridlock and accidents.

3) Grid: The unreliable operations of renewable sources of energy (e.g., solar and wind) create an imbalance between power generation and demand [45]. Plug-in electric vehicles (EV) can be connected to the grid to provide load stability making the grid a part of the IoV. Surplus energy stored from renewable energy sources can be stored in the batteries of EVs and returned to the grid for proper distribution. Connection to the grid is necessary for vehicles to know when and how to request energy. V2G provides such connections to improve the efficiency of the grid for power distribution. Other aspects of the grid include the economics of electric vehicle charging, which involves establishing a robust infrastructure network of charging stations supporting the increasing number of EVs on the road.

4) Homes: Homes are also an essential part of the IoV that benefits from vehicle-to-home (V2H) technology. This technology allows EVs to deliver energy to homes to provide power or back to the grid using bidirectional charging or a V2H charger. V2H technology is another V2G integration, which is about self-consumption to decrease electricity costs and improve network stability. By charging electric vehicles using renewable energy sources and providing power to the home, demand on the grid is reduced, especially during peak hours, and the EVs can become power storage that can act as emergency power backup.

5) Road Side Units: The RSUs provides better communication service when vehicular density is sparse by making use of RSUs as relays to assist in the transfer of traffic messages [46]. Due to the distance limitation of DSRC for V2V communications, vehicles cannot send messages over long distances. In this scenario, RSUs can act as routers to facilitate distant data transfer by enabling multi-hop communication [47]. Also, RSUs are vital in deploying authentication schemes to verify certificates of vehicles in a vehicular network. RSU units can include grids and homes as stated above.

6) Cloud: Data exchange between the cloud and vehicles is enabled by V2C communication. Due to the computational constraints of cars, the cloud can be used for data processing and storage. Machine learning and security measures utilize the computational and storage resources of the cloud for IoV applications [48].

D. IoV Users

In this section, we briefly discuss users in the IoV ecosystem. These users can be broadly classified into: drivers and passengers, government and other public sector organizations, businesses, pedestrians, and emergency service providers.

1) Drivers and Passengers: Drivers and passengers are the first users in the IoV system as they are offered in-vehicle digital experiences and IoT-centric consumer benefits, including comfort-based services, infotainment, and mobility solutions. To ensure a seamless implementation of cooperative intelligent systems, drivers should be able to easily navigate their cars and use vehicular resources.

2) Government and Other Public Sector Organizations: Government organizations set up policies that monitor and regulate road usage. In addition, researchers and manufacturers collaborate with the government to develop standards that facilitate the efficient adoption of vehicular technologies by the public. These standards are developed by international organizations such as the International Organization for Standardization, European Telecommunications Standards Institute, International Telecommunications Union, and Society of Automotive Engineers. In addition, these organizations provide protocols and frameworks that ensure uniformity across the industry and facilitate the implementation of IoV technologies.

3) Businesses: Businesses leverage vehicular technologies and its interaction with IoV nodes to provide services, such as navigation, car-to-home integration, over-the-air updates, and insurance. As an example, user-based insurance (UBI) products are used by businesses to evaluate driving risks. These assess the driving risks of drivers based on various metrics such as fuel consumption rate, the distance covered by the vehicles, acceleration or deceleration rate, time-of-day driving, hard brake events, and high-speed driving. Some businesses providing this product construct a fee, while others provide a discount to premium services. Alternative examples of UBI are pay-how-you-drive and manage-how-you-drive [49]. Other services include smart parking [50], car-sharing [51], remote diagnostics, infotainment, emergency, and location-based services.

4) Pedestrians: Pedestrians require an appropriate time to cross and need to keep a straight heading while crossing intersections. To safely complete the crossing and boost self-confidence on our roads, pedestrians need information about the geometry of intersections, signal timings, and traffic [52]. In addition, vulnerable road users, such as blind and visually impaired pedestrians, have reduced mobility options and need to accomplish specific tasks, including street detection, locating crosswalks, and alignment. These tasks can be achieved with the proper integration of V2P communications. In V2P technology, both vehicles and pedestrians get informed about the presence of one another to improve the accessibility and level of confidence while avoiding collisions [53], [54], thereby removing both physical and mental barriers that could interfere with vulnerable pedestrian mobility. To reduce the risk of collisions and enhance safety, V2P requires a reliable network for timely delivery of messages.

5) Emergency Service Providers: Emergency services provide preventive measures and interventions for situations, such as vehicle crashes and breakdowns, that can pose risks to the life and health of road users. Emergencies could also include circumstances endangering the environment [55] or events that threaten security. During emergencies, providers such as the police, health, and fire services require road access to reach their destinations and offer a timely response to reduce the severity of injuries. The efficient operation of traffic management and seamless exchange of accurate emergency notification—location, number of victims, and severity—across IoV would ensure that these providers respond promptly during emergencies.

IV. Taxonomy of IoV Interoperability Challenges

IoV entities include nodes using different data structures and protocols. The network used by these devices has disparate requirements and implements heterogeneous technologies and communication models. In addition, the dynamic network of mobile vehicular nodes makes it difficult to maintain sustained connectivity that would enhance continuous data and resource sharing among network entities. Interoperability in IoV ensures that nodes, networks, and applications across heterogeneous platforms can interwork to deliver optimal services to users in the ecosystem. IoV interoperability also implies access to vehicular and traffic data via secure communication channels and enhancing middleware platforms that facilitate analytics and semantic processing. To contribute to a more intelligent transportation system and advance social and economic development, the automotive environment requires seamless information exchange, made possible by introducing interoperability into the IoV system that allows for a better workflow and cooperativeness when data is accessed or exchanged between vehicles.

In IoV, the intersection of diverse technologies encompasses data sharing, safety and automation, energy conversion, and reduced congestion on the roads. However, the integration of communicating entities of the IoV with transportation infrastructure is essential as with other sectors, including health care, energy, home, manufacturing, and agriculture, which will be an integral part of the overall smart city ecosystem. IoV interoperability ensures that entities can interwork to support applications and services, and these depend on the acquisition of core technologies and standards to secure strategic advantage. Moreover, achieving interoperability in IoV would enhance V2X communication and ensure that the QoS requirements of the ecosystem are satisfied for the integrated information services of vehicles and their safety.

Here, we present five classes of interoperability in IoV. These categories provide different perspectives on studying interoperability and highlight integration challenges, including access, transfer, and use of data as intended. Fig. 4 shows the classes that emphasize the categories in which interoperability must be achieved to ensure a fully integrated IoV ecosystem, which includes node, network, data, systems, and applications.

A. Node Interoperability

Node interoperability enables the integration of IoV components with supported standards and communication technologies in the ecosystem. However, each node's implementation is not generalizable due to heterogeneity and lack of standards in the ecosystem. As a result, the interfaces of different nodes in the ecosystem must be harmonized to support efficient data exchange and guarantee that the technologies used by each node can interoperate to enable smooth communication. IoV applications run on devices that implement different technologies and require support for a wide coverage area [56]. As new protocols and communication improve the efficiency of these applications, each node should be capable of supporting these protocols and technologies, ensuring seamless access and transfer of usable data in the ecosystem.

Achieving a seamlessly interoperable IoV requires that protocols for the physical (PHY) layers address issues relating to multipath fading and Doppler frequency shifts caused by vehicular mobility. Moreover, the medium access control (MAC) protocols for IoV should support applications with time constraints while addressing challenges related to shared bandwidth among the communicating nodes [19]. To ensure efficient communication of nodes using different wireless standards to define the PHY and MAC layers, protocols such as DSRC that describe integration techniques of wireless standards should be adopted to improve node interoperability. The Third Generation Partnership Project (3GPP) specifies the latest radio-based V2X standard to improve cellular-V2X (C-V2X) communication [57]. However, issues such as reducing complexity and implementation cost persist in achieving interoperable nodes in IoV. Also, the default standard—IEEE 802.11p—suffers from degradation due to hidden terminals and collisions in wide coverage areas [58] given rise to the design of the IEEE 802.11bd standard. For a fully interoperable ecosystem, nodes should be able to communicate using different transmission modes, such as IEEE 802.11bd and IEEE 802.11p, and sufficiently decode data from nodes using other protocols [59]. In addition, standards that ensure the integration of heterogeneous protocols would improve nodes integration, support unified interfaces and efficient protocol translations, and low latency and optimal resource utilization.

B. Network Interoperability

The unification of diverse network topologies in the ecosystem needs to address QoS, mobility support, security, network fragmentation, location awareness, resource optimization, scalability, and routing. Since vehicles in IoV are mobile nodes, the communication network maintains a dynamic topology that makes it difficult to maintain network connectivity. As a result, the network should be resilient enough to support vehicles that constantly move in and out of the coverage area. One of the main concerns of the IoV network is the routing protocol used to pass packets to their destination and the associated cost. During packet routing, the network should be robust while minimizing end-to-end delay and maximizing the resource utilization of the network. Routing protocols used in VANET have challenges related to low scalability, degraded QoS, low energy efficiency, limited transmission bandwidth, and broadcasting issues [60]. These challenges make VANET protocols unsuitable for IoV networks. Routing protocols in IoV must be scalable, stable, and support redundancy while transmitting delay-sensitive and safety-critical packets in the case of network failures or high-density traffic [61] feasible with network support for collision avoidance and alternate routing techniques. Another challenge of IoV communication is non-line of sight issues caused by the blockage of high-frequency signals by obstacles such as trees and buildings in urban environments. This challenge, coupled with the difficulty of efficiently adjusting the congestion window in TCP, causes degradation of the communication reliability in networks, such as 5G millimeter wave (mmWave), which can provide fast data rates and wide bandwidth availability for vehicular communication [62].

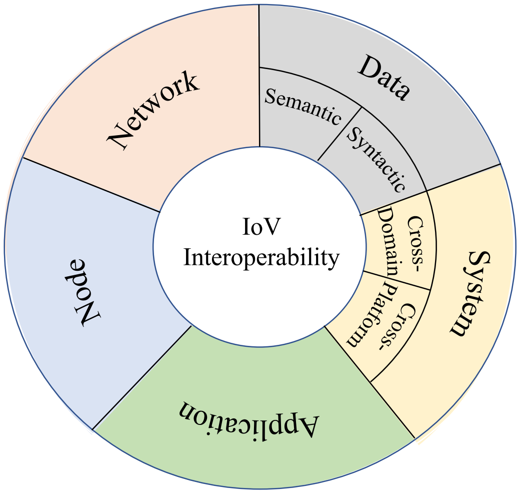


Fig. 4: Classification of IoV Interoperability.

C. Data

Data interoperability ensures that data structures and syntax used in IoV are compatible to ensure unambiguity and shared meaning. Moreover, sharing data in the ecosystem should not create conflict during storage, transfer, and processing. Data interoperability can be grouped into semantic and syntactic interoperability.

1) Semantic Interoperability:: Semantic interoperability ensures that shared data have meaning and are unambiguous. Well-formed semantics enable computers to understand and process data efficiently [63]. An example of an implementation of semantic interoperability is the semantic web, an extension of the world wide web which gives well-structured meaning to data. Other examples of frameworks that facilitate the creation of standardized forms of web data include resource description framework (RDF), web ontology language (OWL), and linked data [64]. Ontology is fundamental to the implementation of semantics. It assists in understanding data and facilitates auto-processing and retrieval of data [65] by providing formal names and defining their relationships with other entities in the network. The capability of IoV to inter-operate semantically could ease the process of creating forensic statistics when

This article has been accepted for publication in IEEE Transactions on Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TITS.2022.3194413

accidents occur. Semantics can also improve the speed of database queries of IoV-related data.

Semantic interoperability requires that the ontologies used to represent data be accessible to participating entities, and the terms defined by different vocabularies present a unified data interpretation by clarifying relationships and providing domain-dependent and independent ontologies [66]. While there have been attempts to define ontologies and vocabularies for vehicular data, the definitions do not adequately represent all the available IoV data [67], [68]. Therefore, the ontologies still require extensions to comprehensively define the sensors, actuators, and signals available in IoV [69]. Also, lightweight ontologies can facilitate the annotation of data with the necessary information that would not overwhelm vehicular resources [70].

2) Syntactic Interoperability:: Nodes that operate with different syntactic implementations need to have methods that ensure compatibility with other syntactic structures. Syntactic interoperability ensures that data are formatted correctly and ready to be annotated with proper semantics. Correct syntax of data is crucial during the usage of differently structured data generated from different devices. For instance, in some operating systems, ‘long int’ is 32 bits, while 64 bits in others [71]. Also, units of measurements or provenance data may present data format discrepancies that make them inefficient for cooperative usage in architectures, such as the Social Internet of Vehicles (SIoV). Hence, data from different entities require defined structures to be accepted by a receiving node. Examples of syntax standards are Extensible Markup Language (XML) and JavaScript Object Notation for web syntax structures. SOAP, RESTful, web services description language, and hypertext transfer protocol are examples of technologies that assist in achieving syntactic interoperability on the web.

Due to the heterogeneous nature of the vehicular network, data from vehicles may need to be aggregated and compressed to reduce message sizes significantly and avoid wireless collisions [72]. The absence of standardized syntactic structures can lead to inefficient analytical results and impact the quality of data used by various IoV applications. Processing data with heterogeneous formats is also challenging, requiring expensive computing resources for efficient query processing. Moreover, a vehicle manufacturer might use different syntax across vehicle make, model, and trim. To ensure the seamless processing of IoV data and enhance the integration of various entities, syntactic solutions to normalize, compress, and efficiently aggregate data from different IoV nodes are essential in the ecosystem.

D. Systems

The ability of heterogeneous systems to interwork ensures that data and resources are shared seamlessly to support IoV applications. Moreover, the compatibility of different systems allows applications from disparate domains and platforms to exchange information, as described below.

1) Cross-Platform Interoperability:: IoV platforms enable the development of software and hardware solutions to support applications. Cross-platform interoperability ensures that applications can run across disparate platforms irrespective of their underlying architecture or operating environments. Considering applications requiring aggregated data for emergency notification to appropriate agencies, such as fire and ambulance services, which run on platforms with different operating requirements, cross-platform interoperability will provide an extensive understanding of proprietary platforms required by developers to ensure applications have access to data across heterogeneous platforms.

To advance the development of vehicular applications, prototyping software and tools supporting different platforms are crucial for integrating vehicular components. However, current frameworks, such as the Robot Operating System and Vector Informatik’s CANoe, have poor support for available operating systems, inadequate automotive resources, and do not offer a robust solution for automotive software development [73]. Furthermore, evaluating and testing real-life applications in IoV may be infeasible, and thus, collaborative and open-source simulation tools that integrate different IoV platforms are necessary. Tools incorporating open platforms for evaluating vehicular systems and supporting efficient application development are essential.

2) Cross-Domain Interoperability:: IoV can operate in two different models, vertical and horizontal, for domain interoperability. In the vertical model, the IoV device, other entities, and services are all provided and managed by the same provider, while the horizontal model allows for multiple providers to interwork with a common framework to promote rapid growth and innovation, resulting in divergent development. Vertical domains such as ITS and smart health have unique collections of entities that share common interests and possess well-built components that are existentially fundamental and only permit changes in a particular dimension. Unlike the IoV, which can have different providers for entities such as connected vehicles, intelligent devices, cloud services, grid, home, and security systems. Cross-domain interoperability facilitates interaction and seamless exchange of information among entities across federated heterogeneous domains. As these unique domains rely on different technical, environmental constraints or protocols and data formats for end-to-end communication, integrated solutions that support cross-domain interoperability are required to ensure data availability to IoV applications. Moreover, these solutions would also ensure that developers can build applications without needing to know internal details of platforms from different domains [74]. For example, domain-specific enablers support the development of innovative cross-domain applications by providing an interface for accessing aggregated data from different platforms in a specific domain to other domains. The use of enablers can ensure that data from a particular domain, such as ITS, is available to applications of other domains, such as smart health [75].

E. Applications

Application interoperability handles communications and interaction between heterogeneous applications and other services, such as shared system resources and middleware services [76]. The application layer services should support adequate abstraction of the underlying technology and provide flexible interaction in the ecosystem. Moreover, applications should be compatible with existing standards and protocols, provide APIs for cross-application inter-activities, and support seamless communication between distributed systems in the ecosystem. The interworking of applications in IoV would reduce data silos and thus, enhance inter-application interactions. Moreover, achieving application interoperability would ensure that safety-critical data can be transmitted faster across platforms, guaranteeing the QoS.

In addition, interactions between users using cooperative IoV applications involve sharing data and exposing sensitive information raising the risk of privacy infringement. Since many applications in IoV depend on vehicles broadcasting beacon messages that include details such as the vehicle's identity and location data, ensuring the anonymity of users is crucial to protecting privacy [77]. Adopting multi-party private set intersection protocols, blockchain technology, and cooperative authentication techniques for data exchange can help improve the users' privacy [78].

V. Interoperability Solutions in IoV

In this section, we describe some of the proposed approaches to handling interoperability in IoV and their functionalities. The proposed methods mainly focused on network technologies that can help with efficient communication in the IoV. Table II relates these approaches to our taxonomy, and Table III summarizes the strengths and limitations of the proposed approaches. In the following, we discuss the proposed approaches and the open research problems.

A. Core Network

Different solutions for core network interoperability have been proposed for IoV, including access gateways, efficient routing protocol, and network mobility (NEMO) approaches.

1) Access Gateways for Heterogeneous Nodes and Network Integration: One way to address interoperability is by using access gateways or adapters that serve as bridges between nodes using different data structures, communication protocols, or specifications. These gateways can be dedicated hardware or included in the firmware of chips to enhance the integration of heterogeneous devices in the perception layer [7], [108]. In vehicular networks, communication gateways can ensure that efficient and secured connections are established between IoV nodes. The gateways enable protocol conversions between nodes and provide mechanisms to manage configurations [109].

Chekkouri et al. [79] proposed a gateway architecture that integrates VANET and 4G LTE-A heterogeneous network for enhanced mobility in LTE-A small cells. In the architecture, a mobile gateway connects vehicles to the 4G LTE-A network, providing a cost-effective solution for V2I communication. In addition, the architecture uses an anchor-based mobility scheme to address mobility issues in the network. This scheme allows vehicles acting as mobile gateways to perform local path switching with an anchor unit while roaming inside neighboring cells. The proposed gateway architecture reduces signaling overhead and improves network stability for vehicular nodes in a dynamic network topology. Kim et al. [80] proposed an IoV access gateway (IoV A-GW) that connects in-vehicle networks such as controller area network (CAN), FlexRay, Media Oriented System Transport, and Ethernet to the broader IoV network. IoV A-GW uses a global IP address and supports communication between vehicles and other vehicles or RSUs. Since transmission efficiency can be affected by the dynamic nature of the IoV network, IoV A-GW has an e-Monitoring state to observe the condition of the external IoV network. In addition, the gateway predicts the state of the external wireless network using an inference function. The monitoring and prediction enable the gateway to steer incoming and outgoing traffic delivered to the IoV through a virtualized network.

Summary and Open Problems: Gateways enable reliable communication between nodes and supports the integration of different network technologies. However, in IoV networks where vehicles have to communicate with other vehicles, RSUs, and the cloud, data in the network is explosive and can lead to an overload where each vehicle require access to the network. In this scenario, the network can become degraded due to transmission delays, packet losses, and inefficient handover techniques in dynamic networks. One way to improve the reliability is through the formations of clusters and the selection of vehicular gateways that transmit data in the network. However, gateways have to be selected appropriately to address signaling overhead, mobility, frequent handovers, congestion, and low coverage issues [79], [110]. Different techniques, such as distributed approaches [111], centralized [112], fuzzy logic [110] techniques, have been proposed to solve the gateway selection problem. However, finding a solution that guarantees optimal network performance for the gateway selection problem is still an open research problem.

2) Routing Protocols: Protocols enable communication among nodes in the network irrespective of their internal architectural designs by providing a set of rules by which data is transferred across the network. Several proposed protocols have focused on solving network interoperability issues by reducing latency, optimizing energy usage, improving security, and increasing packet delivery rates [113]–[117].

Leveraging the advantages of 5G technology, Wang et al. [81] presents a low-latency and energy-efficient routing protocol based on network connectivity (LENC) to achieve high reliability and low latency in IoV networks. Using a non-homogeneous Poisson process for the analysis of the network connectivity, they evaluate the probability of selecting a connection route for vehicular data and supply this probability as one of the inputs to a fuzzy controller. The route lifetime of pair-wise vehicular nodes is used as an additional input by the controller to evaluate the best route for exchanging data. LENC reduces the number of dropped packets in the network, average delay for end-to-end communication, routing overhead, and optimizes energy consumption rate. However, limitations of their approach are the assumption that the communication radius between nodes in the network is fixed and the lack of consideration for heterogeneous networks. Achour et al. [82] propose a simple and efficient adaptive data dissemination

TABLE II: Comparative summary of proposed IoV Interoperability solutions. In this table, the approaches implemented in the examples address the interoperability issues indicated by the check marks

Network Domain	Approaches	Examples	Node	Network	Data		System	
					Syntactic	Semantic	Cross-Platform	Cross-Domain
Core Network	Access Gateways	Chekkouri et al. [79]	✓	✓				
		Kim et al. [80]	✓	✓				
	Routing Protocols	Wang et al. [81]		✓				
		Achour et al. [82]		✓				
		Nam et al. [83]		✓				
		Gasmi et al. [84]		✓				
		Afzal et al. [85]		✓				
		Mershad [86]		✓				
		Omar et al. [87]		✓				
		Attia et al. [88]		✓				
	Network Mobility	Lee et al. [89]		✓				
		Nashaat [90]		✓				
Vehicular Communication Network	Vehicular Delay Tolerant Networks	Ahmed et al. [91]		✓				
		Vieira et al. [92]		✓				
		Er et al. [93]		✓				
	Vehicular Named Data Networks	Guo et al. [94]		✓				
		Yan et al. [95]	✓	✓	✓	✓		
		Ahmed et al. [96]		✓				
	Vehicular Software Defined Networks	Salahuddin et al. [97]	✓	✓				✓
		Correia et al. [98]	✓	✓				
	Social IoV	Smaldone et al. [99]	✓		✓	✓		
		Hu et al. [100]	✓			✓	✓	
		Alam et al. [101]	✓		✓	✓		✓
Distributed Network	Fog and Edge Computing	He et al. [102],	✓	✓				✓
		Zhang et al. [103]		✓				
		Ning et al. [104],		✓				
		Chun et al. [105]		✓		✓		
Decentralized Network	Blockchain	Liu et al. [106]		✓	✓			
		Gao et al. [107]		✓	✓			

protocol (SEAD) for vehicular ad-hoc networks. By using a redundancy ratio, vehicles using SEAD dynamically estimate the rebroadcast probability of messages according to the surrounding vehicular density. With an estimate of message rebroadcast probability and waiting time, each vehicle determines when to forward messages in the network. SEAD implements a simple mechanism that does not require beacon messages and thus, addresses the broadcast storm problem in VANETs.

The stream reservation protocol (SRP) was introduced by IEEE std 802.1Q to provide network flexibility and support resource reservation for real-time traffic [118], [119]. Nam et al. [83] present a simplified SRP over SDN for in-vehicle bridged networks. In the proposed scheme, messages are processed centrally in the network to remove the requirement of bridge-by-bridge propagation in SRP. The approach ensures that reserved flows in the network are protected whenever there is an overload of bridge links.

Gasmi et al. [84] presented a stable link-based zone routing protocol (SL-ZRP) to provide link stability in IoV applications. The proposed approach is an enhanced version of the ZRP, a hybrid routing protocol that divides its network into different zones and maintains the current topological map of the zones using a route discovery procedure. SL-ZRP uses a QoS function based on speed, destination, and delay to discover stable routes, decreasing the response time and network overhead.

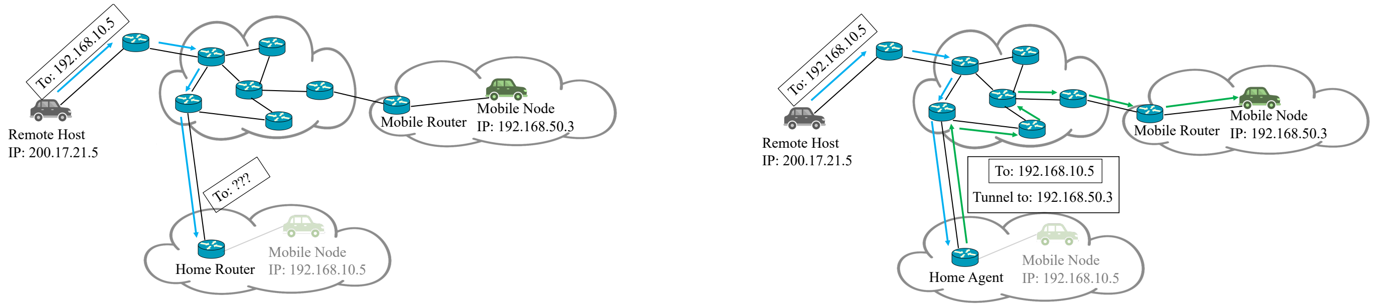
Some of the issues that prevent vehicular communications are the dynamic topology, frequent disconnections, and impediments caused by high-rise buildings. Afzal et al. [85] propose a routing protocol for IoV using unmanned aerial vehicles (UAVs). In the proposed model, the authors allow direct vehicular communications and communication via aerial nodes deployed at different ranges of the vehicle environment. The experiment shows a better packet delivery ratio, reduced end-to-end latency, a lower packet drop ratio, and higher average throughput using the aerial nodes. The authors conclude that

TABLE III: Summary of contributions and limitations of proposed IoV interoperability solutions

Network Domain	Approaches	Examples	Contributions	Limitations
Core Network	Access Gateways	Chekkouri et al. [79]	Integrates heterogeneous VANET and 4G LTE-A for enhanced mobility in LTE-A small cells *Strength:* Low vehicle signaling costs toward the core	The centralized hand-off management technique for mobile nodes in the core network is not efficient for large IoV networks
		Kim et al. [80]	Gateway connects in-vehicle networks to the IoV *Strength:* Reduction in transmission delays	No consideration for the syntax or semantics of transmitted data
	Routing Protocols	Wang et al. [81]	A low-latency and energy-efficient routing protocol based on network connectivity for VANET *Strength:* Enhanced routing stability	The type of network considered is homogeneous
		Achour et al. [82]	Simple, efficient, adaptive VANET data dissemination protocol *Strength:* A flexible protocol for different applications	No consideration for sparse networks
		Nam et al. [83]	Simple SRP over SDN for in-vehicle bridges *Strength:* Resource reservation for time-sensitive traffic during overload	No support for redundancy
		Gasmi et al. [84]	A link-based zone routing protocol for IoV applications *Strength:* Enhanced link stability suitable for IoV	The mobility of nodes is not considered for the network
		Afzal et al. [85]	A routing protocol for IoV using UAVs *Strength:* Higher packet delivery ratio than traditional routing protocols in VANETs	No consideration for end-to-end delay of packets
		Mershad [86]	A secure SDN-based routing protocol that uses a blockchain consensus algorithm for security *Strength:* Enhanced security and packet delivery ratio	Only RSU network is considered
		Omar et al. [87]	An integrated protocol that combines greedy perimeter stateless routing with RL *Strength:* Increasing packet delivery with increasing nodes	No consideration for storage capacity constraints
		Attia et al. [88]	An advanced greedy hybrid bio-routing protocol to optimally forward packets *Strength:* Reduced packet delay and scalable for large network	Only V2V and V2I networks are considered
	Network Mobility	Lee et al. [89]	A cross-layer hierarchical network mobility framework for high-mobility IoV networks *Strength:* Resilient to error-prone packet transmission	No consideration for multiple root-FMAs
		Nashaat [90]	A QoS-aware NEMO for time-sensitive systems *Strength:* Improved handover latency	No consideration for heterogeneous applications such as voice and video applications
Vehicular Communication Network	Vehicular Delay Tolerant Networks	Vieira et al. [92]	A routing strategy using three metrics: sense, distance, and speed, to determine whether data forwarding mechanism *Strength:* Improved routing performance in VANETs	Mobility of source and destination nodes is not considered
		Er et al. [93]	Efficient routing for energy constrained IoT devices *Strength:* Help saving the energy for time-critical applications	Data transfer time between an IoT device and vehicle is not considered
	Vehicular Named Data Networks	Guo et al. [94]	Bayesian receiver forwarding for interest packets *Strength:* Efficiently suppress the broadcast storm problem by helping each node minimize redundant interest forwarding	No consideration for malicious nodes in the network sending a false network status
		Yan et al. [95]	NDN vehicular network architecture for IVC *Strength:* Improved content naming, addressing, data aggregation, and mobility for IVC	The security and integrity of the cached contents are not considered
		Ahmed et al. [96]	A controlled data propagation algorithm for VNDN *Strength:* Reduced data congestion, redundant data, and bandwidth wastage in VNDN	Node mobility and caching overhead are not considered
	Vehicular Software Defined Networks	Salahuddin et al. [97]	An RSU cloud architecture that uses virtualization and SDN *Strength:* Minimizing cloud delays, reconfiguration overhead, number of service hosts, and virtual machine migration	Minimizing control plane modifications has not been considered
		Correia et al. [98]	A hierarchical SDN-based vehicular architecture to handle connection loss with SDN controller *Strength:* Improves performance in lossy networks	Scenarios in which the primary controller is present but assists in network coordination to a limited extent are not considered
	Social IoV	Smaldone et al. [99]	A framework for building virtual mobile communities *Strength:* Establish better communication among commuters	Roads with a large number of cars are not considered during evaluation
		Hu et al. [100]	A social networking system to provide feedback to drivers regarding their driving behavior concerning fuel economy *Strength:* Establish green transportation	A prediction mechanism to predict behavior in advance to control the behavior has not been done
		Alam et al. [101]	A cyber-physical architecture for the Social IoV *Strength:* Support for safety, efficiency, infotainment and comfort applications in Social IoV	No consideration for practical deployment
Distributed Network	Fog and Edge Computing	He et al. [102]	A software-defined cloud/fog networking (SDCFN) to achieve load balancing in IoV fog networks *Strength:* Support for latency-sensitive services in IoV	No consideration for security and storage capacity
		Zhang et al. [103]	Caching for mobility-aware vehicular edge networks *Strength:* Enhanced cache utilization and energy efficiency	Does not include all relevant IoV nodes
		Ning et al. [104]	Task offloading and content caching for dense vehicular networks *Strength:* Enhanced offloading and edge caching for RSU	No consideration for data reduction techniques to improve caching in resource-constrained edges
		Chun et al. [105]	Semantic representation of IoV data in fog networks *Strength:* Support for publish/subscribe of semantic information among fog nodes	No experiment was carried out with real-world IoV data
Decentralized Network	Blockchain	Liu et al. [106]	Performance optimization of blockchain-enabled IoV networks *Strength:* Improved throughput in blockchain-enabled IoV networks	No consideration for adaptive consensus algorithms that can handle different network scenarios in IoV
		Gao et al. [107]	A combined blockchain and SDN architectures for Fog and 5G IoV environment *Strength:* Enhanced trust management in fog and 5G IoV networks	Comparison with other routing protocols in terms of efficiency and trust has not been conducted

using aerial nodes improves routing performance.

Mershad [86] proposed SURFER, a secure SDN-based routing protocol that uses a high-performance blockchain consensus algorithm for security. SURFER incorporates SDN to improve ROAMER that relied heavily on the RSU network for communication. ROAMER combined geographic and carry-and-forward strategies providing better performance in sparse and dense conditions but lacking secure communica-



(a) Routing without NEMO: Remote host sending packet to mobile node using its old IP address. Home router does not have a clue on where to drop the packet.

(b) Routing with NEMO: Mobile router of the new network keeps updating home agent about the new IP address. If a packet is received by the home agent of the node, it is tunneled to current IP address.

Fig. 5: Routing of mobile nodes while changing location with and without NEMO

tion. SURFER secures messages by introducing blockchain for each type of transaction. The architecture performs best when inter-communicating distances between vehicles are high.

Omar et al. [87] presented GreedLea, an integrated protocol that combines greedy perimeter stateless routing (GPSR) with reinforcement learning (RL) to determine the message route and forward data in the IoV network. The greedy approach evaluates the shortest routing path using a table from a neighboring node, while the perimeter mode uses a graph to plan the network topology. Since the greedy approach may sometimes fail to find the shortest path, the perimeter mode provides redundancy to the system in case of failure. In addition, GreedLea leverages RL to develop a mobility model for the vehicular network to optimize message routing while minimizing the risk of road collisions. The proposed routing protocol manages dynamic networks to reduce packet loss during intermittent and sparse connectivity. Also, Attia et al. [88] proposed an advanced greedy hybrid bio-routing protocol that uses the greedy road selection (GRS) and hybrid route setup procedure (HRSP) to optimally forward packets. The GRS enables vehicles to forward packets using the shortest possible routing path. The HRSP uses an artificial bee colony algorithm that allows nodes to choose a forwarding route that guarantees packet delivery with minimum latency using criteria such as the direction of travel, bandwidth, and delay.

Summary and Open Problems: Approaches focusing on routing protocols improve network interoperability by using algorithms that support node mobility and resource optimization through techniques such as route selection, energy consumption rate, road segment evaluation, and packet retransmission improvement. However, the need for scalable algorithms that ensure QoS and security in IoV requires further investigation, especially for extremely dense or sparse environments. In addition, the protocols discussed have considered a homogeneous network where vehicles use the same communication technologies. For example, nodes in the work of Balasubramanian et al. [120] use WiFi technology for communication. However, this is not the case in real-world IoV networks where entities use different technologies for end-to-end communication. The development of protocols that provide reliable communication, reduce broadcast flooding, enhance route optimizations, and guarantee data delivery are needed to improve network interoperability in large-scale heterogeneous IoV networks. Moreover, as vehicles move in and out of a network's coverage area, algorithms that ensure quality hand-off techniques are required to maintain network connectivity while maintaining the QoS requirements of a dynamic network.

3) Network Mobility: NEMO is a standard developed by the Internet Engineering Task Force (IETF) to enhance communication among mobile nodes that can be used to optimize data sharing and routing for IoV interoperability. As an extension of Mobile IP [121], NEMO allows vehicles to access the Internet by using tunneling techniques between a mobile router (MR) and a home agent (HA) as shown in Figure 5. MRs act as default gateways and manage the mobility of nodes in the network. Each MR maintains network connectivity by receiving a Care-of-Address (CoA) whenever it moves from its home link to connect through a visited link. The CoA is then registered with the HA, which creates a binding entry that enables traffic to be routed to the desired node [122]. NEMO allows the integration of networks belonging to different administrative domains, such as V2V and V2I, by using nested networks [123].

Lee et al. [89] present a cross-layer hierarchical network mobility framework (Hi-NEMO) to improve the quality of handover techniques for high-mobility IoV networks. The authors introduce a foreign mobile agent module (FMA) which is installed in routers. Whenever the process of handover is initialized and a target BS has been determined, the FMA ensures that packets are delivered quickly by enforcing quality hand-over approaches. While NEMO provides handover procedures to ensure connectivity in vehicular networks, it does not have route optimization techniques that improve latency reductions for heterogeneous vehicular networks [124].

Another example of the implementation of NEMO is presented by Nashaat [90]. In the approach, a QoS-aware NEMO protocol is used to enhance the QoS requirements of time-sensitive systems. The NEMO protocol interwork with layer 2 of WiMAX technology to support fast handover without replacing the traditional handover approach of the WiMAX. The protocol supports reduced network latency and minimal packet loss by combining resource allocation with mobility management.

Summary and Open Problems: The implementation of handover procedures in mobile networks is crucial to achieving optimal packet delivery rates, reduce tunnel overhead, and the

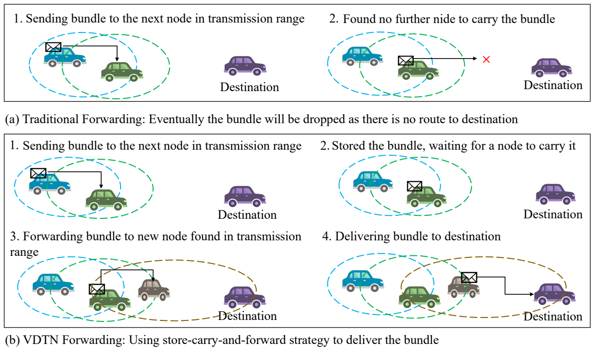
This article has been accepted for publication in IEEE Transactions on Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TITS.2022.3194413

cost of using multiple paths for IoV interoperability. NEMO improves handover techniques by ensuring that network management is not handled by the mobile nodes themselves. However, the procedure for handover introduces an overhead resulting in an increased latency in the network. For time-sensitive applications in vehicular networks, this latency may prevent packets from meeting their deadlines. The architecture requires algorithms that reduce handover latency to ensure consistent connectivity in the network. In addition, since network management is independent of devices, NEMO enables cross-domain interoperability between devices in different administrative domains. However, to ensure that devices in vertical networks can interwork efficiently to support IoV applications, nodes in the network also need to support proper semantic approaches and provide APIs that ensure seamless data exchange and conversion between nodes.

4) Hierarchical Architecture Approaches: Designing a hierarchical architecture that integrates heterogeneous networks is challenging due to the requirements of reliability, modularity, interoperability, and scalability. Also, the architecture should support the integration of IoV with service oriented architecture (SOA), Internet, and interfaces with plug-and-play features [3]. To address interoperability in IoV, different work have proposed layered architectures [3], [21], [22].

Kaiwartya et al. [3] proposed a five-layer architecture including perception, coordination, artificial intelligence, application, and business layers. The perception layer collects vehicular information such as engine condition, vehicle density, and environmental conditions. The function of the coordination layer is to universally virtually coordinate heterogeneous networks and manage the transfer of information from the perception layer to the artificial intelligence layer that serves as the brain of the architecture used for decision making. The application layer provides services to IoV users while the business layer predicts strategies that support businesses. Liu et al. [22] proposed a four-layer IoV architecture that addresses flexibility, agility, reliability, and scalability challenges in IoV networks. The layers include application, control, virtualization, and data layers. SDN controllers are used as the backbone of the control layer and connect the cloud with internet services. Also, the controllers communicate with IoV applications and the virtualization layer that supports the abstraction of data nodes as fog nodes provide storage, computation, communication, and networking capabilities.

Summary and Open Problems: Although hierarchical approaches support the integration of different aspects of the IoV network and support a flexible and agile infrastructure, technologies that guarantee low transmission delays are still necessary for safety-critical IoV tasks with real-time constraints. For example, new technologies such as the 5G or 6G can provide low latency and help to reduce delays in the network. Considering the development of 5G and C-V2X networks, Ji et al. [125] proposed a layered architecture consisting of four layers: security authentication, data acquisition, edge, and cloud platform layers. However, further work is required to integrate IoV with the emerging 5G and 6G technologies to ensure that the QoS requirements of the network are satisfied. In addition, although the addition of an AI layer improves data processing and decision making in the network, there is a lack of adequate protocols for vehicular cloud computing and big data analysis that would ensure the full implementation of AI for data processing in IoV [3].


1. Sending bundle to the next node in transmission range
Destination
2. Found no further nide to carry the bundle
×
Destination

(a) Traditional Forwarding: Eventually the bundle will be dropped as there is no route to destination

1. Sending bundle to the next node in transmission range
Destination
2. Stored the bundle, waiting for a node to carry it
Destination
3. Forwarding bundle to new node found in transmission range
Destination
4. Delivering bundle to destination
Destination

(b) VDTN Forwarding: Using store-carry-and-forward strategy to deliver the bundle

Fig. 6: Traditional forwarding vs VDTN network forwarding

B. Vehicular Communication Network

Different approaches have been proposed to support efficient communication in vehicular networks. Some of these approaches are summarized below.

1) Vehicular Delay Tolerant Networks (VDTN): Traditionally, in TCP/IP networks, packets are discarded in the absence of a link between the source and the destination. In delay tolerant networks (DTN), packets are retransmitted by establishing an alternative path to send the packet on time. Using a store-carry-and-forward strategy, DTN resolves disruptions in the network by sending packets to recipients through intermediate nodes [126]. If it fails to find an immediate node in the network to forward the packets, intermediate nodes store them in the form of bundles in the bundle layer of the DTN architecture. The bundle layer allows DTN to forward bundles irrespective of the underlying network technology. This forwarding approach is depicted in Figure 6.

VDTN assists in extending DTN to vehicular networks by using mobile nodes to carry and deliver data to remote terminal nodes. End-to-end connections between source and destination are rare in dynamic vehicular networks. Intermediate nodes in VDTN are stationary and are placed at different road intersection points. Several routing protocols have been proposed for VDTN such as probabilistic bundle relaying scheme, distance-aware routing with copy control, and adaptive carry-store forward. These protocols improve network connectivity, reduce delay in message delivery, reduce the routing of redundant data and optimize the utilization of routing channels [91]. In VDTN, efficient opportunistic routing protocols must be developed because of the dynamic nature of connectivity among mobile vehicles. Additionally, since relay nodes ought to store and forward data, there is a need to create a management scheme for organizing cached data.

Vieira et al. [92] proposed a routing strategy that uses a benchmark named trend of delivery (ToD) to improve routing performance in VANETs. ToD uses three metrics—sense, distance, and speed—to determine whether data should be forwarded or stored. Maintenance messages that use adaptive detection coverage dissemination scheme is used by ToD to predict how long vehicles in the network will be connected [127]. To manage the buffer in relay nodes, a priority scheme is created which keeps messages with higher priority and discards other messages when it is necessary to drop packets. In comparison to other DTN routing protocols, such as probabilistic routing protocol using history of encounters and transitivity [128], epidemic [129], and spray and wait [130], ToD improves the rate of packet delivery and maintains a lower overhead.

Er et al. [93] use the store-carry-forward mechanism of VDTN and propose an efficient routing solution for energy constraint IoT devices. Delay-tolerant applications such as collecting temperature or air pollution data and images of road degradation get data generated and delivered by low-energy sensors and nodes. The authors introduce DC4LED (Data Collection for Low Energy Devices), where the vehicles such as cars, buses, and taxis will collect, store and transmit data from sensors to servers of the applications. This simple routing mechanism will help the energy constraint IoT nodes save the low-energy for applications where the delay is not preferable such as collecting road accident data.

Summary and Open Problems: Packet delivery is affected in mobile networks and is characterized by intermittent network connectivity. VDTN improves the delivery of packets in vehicular networks by using the “store and forward” approach to keep copies of forwarded data in intermediate nodes. Also, the support for semantics in the bundle layer ensures that data are transferred efficiently between heterogeneous networks. However, due to the copies of packets stored in the bundle layer of the network, VDTN requires enough storage resources that may not be available in sparse networks. The development of efficient data management schemes is needed to ensure the efficient use of available storage resources in the network, resulting in improved IoV interoperability.

2) Vehicular Named Data Networking (VNDN): The requirement of nodes to have IP addresses for end-to-end communications in TCP/IP networks is a limitation for mobile networks such as IoV because of the lack of stability in routes to nodes due to their mobility. Named Data Networking (NDN) is an information-centric networking architecture that tries to address this limitation by making data an independent entities that are separate from the communication channel. In an NDN architecture, nodes can directly request data from anywhere in the network regardless of which node holds the data. A combination of content store (CS), forwarding information base (FIB), and pending interest table (PIT) enhances efficient communication in the network while using every available network path. Moreover, naming data allows NDN to directly secure transmitted data at the network layer making every packet verifiable, which improves the overall security of data and optionally confidential [131].

As shown in Figure 7, a router in NDN architecture checks if the data in its CS matches an interest packet sent by any node. The router checks and records the interest’s name in its PIT table if there is no match before forwarding the interest packet to the producer of the data using information in its FIB. If an interest matches the data in the router’s FIB, the data packet is sent back to the node through the same or different path of the interest packet [132].

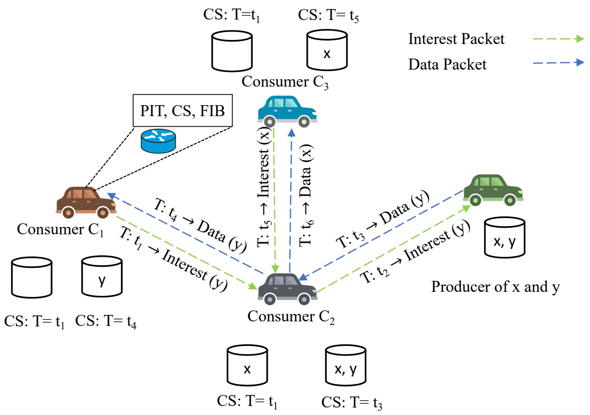


Fig. 7: Simplified forwarding mechanism in VNDN. At time t_1, consumer C_1 Interest packet to consumer C_2 is y. C_2 as no match found in CS, then forward the Interest to the producer of y. Producer send the data y to C_2. C_2 update its CS and forward the data packet to C_1. At time t_5, C_3 forwards an Interest packet requesting for x to C_2. C_2 has a match in its CS and send the data directly to C_3, without contacting the producer.

Guo et al. [94] studied VNDN and proposed a Bayesian-based receiver forwarding decision scheme to solve network congestion formed due to interest flooding. Here, nodes in a VNDN must share their operating status information with neighbors periodically, and the Bayesian model assists each node in deciding whether or not to forward packets using network status information. This scheme helps nodes minimize redundant interest forwarding, reducing network congestion.

Yan et al. [95] proposed an NDN-based vehicular information network architecture to support a single vehicle and multiple nodes in a NEMO network. Their work is based on NDN’s content management framework, communication strategy, and caching scheme. In their approach, data are named based on their location information and the devices producing them. The forwarding strategy in the network is based on the location information that is saved in each interest packet and the data packet. Furthermore, hierarchical aggregators (e.g., city, district, and street levels) aid to collect from multiscale geographical locations. The aggregators process and disseminate the resulting data to connected nodes in the network. Vehicular applications such as infotainment, emergency broadcasts, and traffic management can be supported in the network using these processed data.

Ahmed et al. [96] proposed a controlled data propagation algorithm (CONET) for VNDN. Their algorithm was used to reduce data congestion, redundant data, and bandwidth wastage in VNDN. To keep track of the hops traveled by each interest packet, CONET allows a hop-count field to be added to the interest packet by every node. If the hop-count field is less than or equal to the time-to-live (TTL) value in any node’s PIT entry whenever a data packet arrives, the packet is forwarded to the requesting node in the network; otherwise, the packet is dropped. CONET ensures the delay between the generated interests and retrieved data is improved. Furthermore, it reduces the number of data packets sent

This article has been accepted for publication in IEEE Transactions on Intelligent Transportation Systems. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TITS.2022.3194413

across the network while making sure that interest packets of requesting nodes are satisfied.

Summary and Open Problems: The information-centric framework of VNDN enables the implementation of efficient data management schemes improving interoperability among IoV nodes. In addition, the hierarchical name structures ensure that exchanged data are annotated with information essential to IoV applications. However, the solutions discussed above impose several challenges that need to be addressed further. In the work of Guo et al. [94], the proposed Bayesian model-based scheme provides decisions based on the information shared by the neighbors of each node. The Bayesian model can generate wrong decisions if any malicious node in the network sends a false network status. This may cause congestion in the network initiating the denial-of-service attack. The hop count mentioned in the work of Ahmed et al. [96] is susceptible to changes due to mobility in VNDN. As a result, a hop-count mismatch may prevent the consumer from receiving the data. Since IoV nodes have resource constraints, caching every content may result in additional overhead. The work discussed above does not provide effective caching methods suited for IoV nodes. Research efforts need to be directed towards efficient caching schemes, the privacy of data producers, and mobility management in IoV.

3) Vehicular Software Defined Networking (VSDN): Software-defined networks enable the development of network switches and routers that can run network management programs. These network devices can be used to support applications in distributed systems and heterogeneous network architectures [133]. A basic architecture of SDN is shown in Fig. 8. SDN separates a network's data plane, which manages data forwarding based on control plane logic, from the control plane that handles how packets should be forwarded. This separation is actualized with the use of software programs called "controllers" to directly supervise heterogeneous and distributed programmable network entities through a defined communication protocol, such as OpenFlow [134]. The SDN controller directs traffic according to the implemented forwarding policies that improves the network flexibility by separating network policies from their implementations in hardware [135]. Functions of on-board units (OBUs) in vehicles, such as power control, interface selection, and packet forwarding, allow them to be suitable for the implementation of SDN. Some of the functions that are enabled by SDN in IoV include packet transmission control, network virtualization, and vehicular access hand-off process.

Salahuddin et al. [97] proposed an RSU cloud architecture that uses virtualization and SDN to meet the demands of vehicular networks. The architecture consists of microdatacenters, which are modified RSUs that support SDN and virtualization, and traditional RSUs that communicate with OBUs in vehicles. Due to the need for the reconfiguration of RSUs for microdatacenters, the latency of services increase, which can be reduced by using the proposed cloud resource management scheme (CRM). Delays in the cloud infrastructure are calculated by computing edge delays along a path. To minimize these cloud delays, overhead caused by reconfiguration, and the number of service hosts, the CRM problem is modeled using multi-objective integer linear programming (ILP) and solved to obtain a pareto optimal frontier of non-dominated solutions. Finally, a heuristic is developed to solve the CRM problem and a reinforcement learning approach with Markov decision process is used to select an appropriate configuration that minimizes migrations of virtual machines in the network.

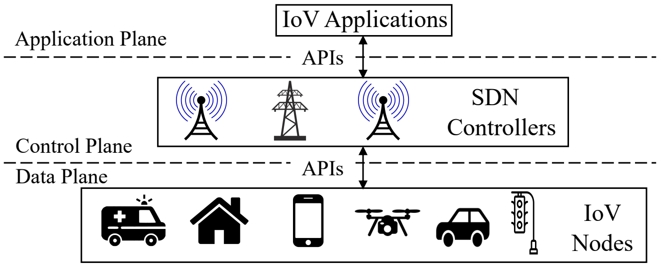


Fig. 8: Simplified view of a three-layer SDN architecture. In IoV, vehicular nodes and other entities in the network infrastructure are supervised by SDN controllers which can be implemented in RSUs to support IoV applications.

Correia et al. [98] propose a hierarchical SDN-based vehicular architecture to address the issue of losing connection with the central SDN controller due to the high mobility of vehicles. Considering the mobility of the vehicles, the authors focus on improving the efficiency and performance of the network when a connection loss occurs. The authors use the clustering concept and create local SDN domains. Each domain will have a local SDN controller with hierarchical access to the central SDN controller. These local SDN controllers contain some of the network intelligence to provide required SDN functionalities when the central controller is unreachable.

Summary and Open Problems: Being traditionally reliant on network hardware, SDN enables traffic management through the use of software-based controllers. As a result, we gain the flexibility to customize network infrastructure, provide dynamic controllers to oversee different networks, and even provide an improved level of security to critical network clusters. However, SDN requires scalable architecture design and proper semantic implementations that support interoperability in IoV applications. Due to the heterogeneous nature of IoV entities, virtualization and abstraction of network resources are required to aid the development of efficient resource scheduling algorithms for SDN-enabled IoV applications [136].

4) Social Internet of Vehicles (SIoV): One of the architectures that promises to aid data management in IoV is the Social Internet of Vehicle Architecture. SIoV is an extension of Social Internet of Things (SIoT) architecture where independent social relationships are established among objects, such as smart phones and smart watches, in a network [137]. Some of the relationships among objects include parental, co-location, co-work, ownership, and social. These relationships are established and maintained by the objects themselves to facilitate effective interactions [138]. SIoV extends SIoT to converge vehicular networks with the social networking paradigm by using the social relationships among physical vehicular network entities to store data, facilitate communication, and encourage interactivity [101]. The first use of a vehicular social network (VSN) was in RoadSpeak [99], which allowed

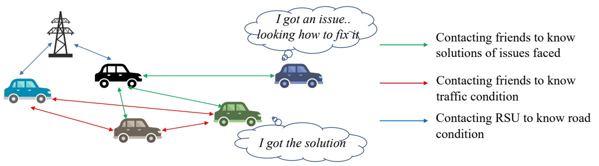

I got an issue..
looking how to fix it
I got the solution
Contacting friends to know solutions of issues faced
Contacting friends to know traffic condition
Contacting RSU to know road condition

Fig. 9: Relationships created by vehicles in SIoV scenario

drivers to join voice chat groups to interact with each other. To limit group admittance to commuters, a threshold based on location and time was used to restrict group membership to specific road segments and time intervals. Hypertext Transfer Protocol Secure (HTTPS) was used for user management in the framework to ensure syntactic interoperability. Moreover, developers can extend the functionality of RoadSpeak using Java APIs. The concept of VSN was also utilized by Hu et al. [100] to develop a social drive system that provided feedback to drivers regarding their driving behavior with respect to fuel economy. The system uses a mobile application configured to upload information concerning driving behavior to Facebook. Storage and management of aggregated data are done using an SQLite database which provides seamless interactions between geo-based services and the social drive application. The approaches discussed bridge the gap between different network protocols and also enable seamless data exchange between traditional IoT and vehicular networks. To ensure semantic interoperability in SIoV, Alam et al. [101] utilizes vehicular ontologies, advanced traveler information system schema and SAE J2735 message set in their proposed architecture. In their work, messages are encoded using XML, and communication among vehicles, RSUs, and the cloud is completed using web RESTful principles where objects are identified using uniform resource identifier (URI). The architecture allows vehicles to create social relationships that can be used to develop innovative applications to assist in ITS.

Summary and Open Problems: SIoV encourages vehicles to share information through social interactions and enables collaboration among different network components to support IoV application. The architecture provides smooth communication among IoV nodes by storing social relationships within the objects themselves and is achieved using context-aware data management techniques. SIoV at present lacks a canonical design agreeable across the vehicular industry [139]. Hence, besides the challenges posed by the heterogeneous and dynamic IoV network, there is a need to develop standard frameworks that provide a basis for the development of SIoV [140].

C. Distributed Network

Distributed networks enable tasks to be shared across different nodes to improve the computational power of the network. An example of a distributed network for vehicular nodes is the fog and edge computing network.

1) Fog and Edge Computing: Conventional cloud computing fail to meet the demands of low latency, geographically distributed, and real-time safety-critical applications in IoV. Fog computing solves these challenges by bringing computation to the edge of the network, as shown in Figure 10.

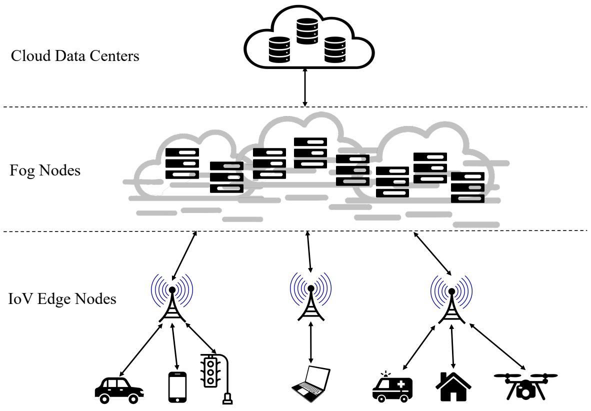


Fig. 10: Fog Computing using IoV Edge Nodes

Fog computing can also provide computing power, storage resources, and communication services between vehicular nodes and the cloud on a highly virtualized platform [141]. He et al. [102] proposed software-defined cloud/fog networking (SDCFN) to achieve load balancing in IoV fog networks. In their approach, IoV is classified into cloud computing, SDN control, fog computing, and infrastructure layers. BSs and RSUs make up the fog computing layer in the architecture. These entities cache and receive information from the cloud and other nodes in the network. Load distribution is modeled as an optimization problem using a modified constrained particle swarm optimization to ensure that optimal load balancing is achieved in the network by SDN controllers. The SDN controllers then inform other nodes of the strategy by forwarding flow tables. The limitation of their approach is the lack of consideration for security and other QoS metrics.

In fog networks, edge caching ensures that the content can be retrieved with reduced latency by vehicles from edge servers. However, caching algorithms must be designed to overcome the challenges of node mobility and dynamic content requirements in IoV networks [48]. Zhang et al. [103] proposed a caching scheme for vehicular networks that considers mobility of nodes in content-centric networks. To evaluate the availability of the network of mobile users, the interactivity between mobile users and caching nodes in the network was modeled using a 2-D Markov process. Based on this model, the efficiency of energy used in the network was formulated as a fractional optimization problem. The optimization problem was solved using Lyapunov optimization theory and fractional programming. The solution facilitate efficient caching with optimal energy use. Ning et al. [104] also proposed a task offloading and content caching scheme that improves RSU-to-RSU and vehicle-to-RSU offloading and edge caching in dense vehicular networks. To reduce delivery delay during prolonged energy usage, caching was modeled as a mix integer non-linear programming (MINLP) optimization problem that is solved using Lyapunov optimization theory. Their scheme was further optimized using support vector machines (SVM) and dataset aggregation techniques.

One way to improve interoperability between horizontal domains—a domain that allows for novelty to occur that results in divergent development—is to introduce semantic annotations for data exchanges in the network. A common approach would be to use ontology such as the OWL to provide semantics [142]. Chun et al. [105] use domain ontology to implement semantics and extract knowledge from processed data in fog architecture. Here, resources in the network get annotated with semantic information grouped as specific events when triggered by some active rules. After these events are detected, a propagator sends them to cloud resources or other nodes that have subscribed to them in the network.

Summary and Open Problems: By bringing computation to the edge, fog computing enables real-time applications to have timely access to data. The support for semantic annotations in fog computing ensures that IoV networks can support applications across heterogeneous domains. Moreover, collected data are processed close to data sources to improve latency for real-time applications [143]. However, fog computing still requires the development of efficient task allocation, resource discovery, data reduction, and caching techniques to achieve a fully integrated ecosystem. Individual nodes lack computational resources and are not efficient for processing large data, which is typical in IoV [44]. Hence, necessary data reduction techniques and distributed computing schemes are vital to improving the efficiency of fog networks to ensure improved interoperability at the cloud and fog layers.

In dense vehicular networks, the use of static mobile edge computing servers can lead to a situation where service requests from vehicular nodes to edge servers impede the quality of the network. The integration of C-V2X, edge computing network, and the emerging 5G/6G technology is crucial to achieving a network that consists of heterogeneous entities that can interwork to deliver service to end-users while maintaining the network quality. Also, the design of efficient protocols for edge networks is crucial for sustained connectivity and efficient spectrum resource sharing in dense vehicular networks [144]. Since edge servers have limited resources compared to traditional cloud servers, it is necessary to find solutions that will optimize edge computation offloading, resource utilization, and reduce network delays in edge networks. Different approaches, such as distributed [145], Lyapunov [104], [146], and AI-based algorithms [147], have been proposed to solve the optimization problem of vehicular edge networks. However, further work is required to obtain an optimal solution that guarantees the best performance for QoS-oriented services and support adaptive resource allocation [22].

D. Decentralized Network

In a decentralized network, no single node controls the network. However, each node contributes its resources independently to perform data processing and decision-making. An example of a decentralized network is the blockchain.

1) Blockchain: Blockchain was introduced to address the “double-spending” problem of digital currency by using peer-to-peer networks (P2P) [148]. Unlike client-server networks, nodes in P2P can act as both a server and a client [149]. P2P architecture allows the network to be decentralized, where there is no defined hierarchy and nodes can assume dynamic roles to perform computational tasks without a central authority [150]. Hence, the architecture addresses the challenge of a single point of failure associated with centralized architectures [151]. Furthermore, P2Ps ability to support decentralized networks enables nodes to make transactions without trusting each other, achieved through a software application that acts as intermediaries between users connected over the internet. The technology makes use of different tools such as timestamps, a consensus algorithm, digital signatures, and economic incentives [152] to perform these transactions. The open architecture of blockchain allows distributed nodes to retain a copy of completed serialized transactions in the network. These transactions are organized in blocks and chained using digital signatures to ensure immutability [153]. Due to its data management and security schemes [154], the application of blockchain to solve security problems between heterogeneous nodes in IoV has been a core research area in recent years. For example, Liu et al. [106] used deep reinforcement learning (DRL) to determine block producers and modify the size and time interval of blocks to maximize transactional throughput in an IoV network based on blockchain. Considering vehicles using 5G in a fog computing paradigm, Gao et al. [107] explores the possibility of data management using SDN and blockchain. In their approach, RSU hubs serve as block miners and an appointed leader among them is responsible for creating blocks. These blocks are verified using the practical Byzantine fault-tolerance consensus algorithm. The use of blockchain in their work helps to alleviate network management loads on SDN controllers and improves the use of available network bandwidth.

Summary and Open Problems: Blockchain improves data management by providing a decentralized framework and offering features, such as immutable digital signatures. However, implementing blockchain in dense vehicular networks may lead to a reduction in network and data throughput for IoV interoperability. Delays in dense networks constrain vehicles to retain an outdated transaction chain that will have to be dropped to accommodate for the single correct chain. [155].

VI. Open Research Challenges and Future Directions

Although significant effort has been devoted to addressing interoperability challenges in IoV, the development of novel approaches that would enable a seamless integration of devices and resolve real-time core challenges are of continuous research interest. Since IoV is still in nascency and the overall scope of unique technologies involved are evolving, emerging technologies that will advance the realization of a fully integrated, secure, and interoperable IoV ecosystem are still in an early developmental stage. We describe in this section some of the open research challenges that still need to be addressed and suggest ways to address them as future directions for research.

A. Standardized Data Syntax and Semantics

The solutions we surveyed offer varied approaches to data management. However, these methods often provide inconsistent data syntax, semantics, or none. A standardized schema is needed to address this challenge to ensure a formal data syntax across the IoV ecosystem. Standard schema is essential to address discrepancies in data syntax for efficient context extraction. The combination of data normalization and data fusion techniques with the development of distributed data analytic modules that efficiently handle noise removal and error correction can assist in handling data with different syntax to support IoV applications [156]. Also, technologies like web semantics are required to create ontologies that could help in providing unified data formats for multimodal IoV data. Furthermore, open APIs that allow devices operating in different domains to interact would aid cross-platform data exchange among IoV applications.

B. Scalability

IoV demands scalable solutions since the cost required to create or change a solution undermines the reasoning supporting its adoption. Also, the network contains various vehicular nodes and deployment environments to process data and assure sustainable service, which requires high scalability in design technology, i.e., architectures that can transition between centralized and decentralized control modes depending on network demands [157]. Solutions must be robust, reliable, and scalable enough to handle rapidly changing traffic conditions in a dynamic IoV environment, and services to manage, share, and secure connected device data intelligently should be standardized while reducing operational costs. Apart from creating a standardized scheme for storing vehicular data, such as the cloud platform, flexible and optimized search engine designs are required for handling requests and retrieving data needed by connected nodes. Moreover, for dynamic networks where nodes can join and leave the network at any time, efficient admission algorithms need to be developed to reduce the latency of joining a network and accepting node requests.

C. Integration With New Technologies

The fifth-generation, sixth-generation networks (5G and 6G) and mmWave provide better connectivity with higher data transmission rate, reduced communication delay, strong detection capabilities, and improved security for networks requiring low latency [158], [159] such as the IoV. Understanding these technologies in terms of channel measurements in dynamic environments, impacts of signal obstructions, and the dynamics of antenna directionality are crucial to their integration for supporting vehicular applications [160]. Integrating these technologies with existing vehicular networks such as Cellular V2X, WiMax, DSRC, and architectures like NDN, SDN, and SIoV would improve QoS for the IoV. However, the interaction of these technologies with existing ones increases the data available for channel measurement, making data processing and understanding the nature of communication channels challenging. Leveraging deep learning algorithms such as generative adversarial networks can improve wireless channel modeling and enhance data management [161].

D. Cross-Domain Integration

Integration of varied domains such as smart homes, ITS, and health enables innovative application development that further improves the availability of services to users in the ecosystem. Applications and services offered by existing vertical domains need to be supported by others implementing different communication protocols and QoS requirements. However, solutions in these domains are developed in silos, making it difficult to achieve interoperability. Integration across platforms and domains requires that manufacturers agree to Standardized framework for intelligent devices production. Also, data access should be seamless across platforms by using a unified interface provided via APIs and resource discovery tools similar to the BIG IoT API for generic IoT platforms [162], [163]. The adoption of vertical silos for IoV platforms and access to domain-specific interfaces is also required to encourage collaborations among heterogeneous domains and enhance cross-platform access to data.

E. Trust Management

The communicating entities in the IoV require a level of trust to interoperate on shared contextual information in the network. Due to the requirement for frequent updates by trust evaluation algorithms trying to reduce the risk of untrusted nodes in the network, the storage and computation of trust-related information create overhead that causes latencies in nodes with constrained computational and storage resources. To address this challenge, scalable and efficient algorithms that formalize and optimize entity reputation and available resources are needed for trust management for information credibility. Furthermore, the design of trust management models should consider semantic interoperability, while solutions leveraging the decentralized capability of blockchain are promising approaches that can provide a secure framework for efficient and scalable trust management [164], [165].

F. Security

The proliferation of electronic devices in modern vehicles has culminated in requiring more than locking physical doors and windows of an automobile for protection. Security is one of the major concerns for automotive manufacturers and technology enthusiasts in realizing a fully interconnected IoV ecosystem. Vehicles are an attractive target to cyber attackers as they can exploit data gathered from a vulnerable car for malicious mischief. Information exchange and computationally intensive tasks in the IoV are performed through wireless media that open the ecosystem to the risk of intrusion. Moreover, different entities connected to the traditional communication network also raise security issues. Although the composability of IoV platforms improves data management in IoV infrastructure, integration of these platforms increases vulnerability to cyber attacks. Security measures—cryptography for application data transfer—and other approaches that do not impact the QoS of IoV infrastructure are necessary to guarantee secured packet delivery in the network.

G. Artificial Intelligence

AI approaches, such as deep and reinforcement learning techniques, help improve the cognitive performance of IoV applications and address complex challenges such as routing, resource management, and task offloading. IoV nodes can leverage AI techniques to learn how to make intelligent decisions to improve safety and resource utilization in the network. However, using AI approaches in IoV is far from trivial as they heavily rely on data from sensors that can be affected by complex traffic conditions, poor stability of network topology, and electromagnetic interference due to natural or human-made sources. For example, snow can cause clustering and tracking issues that impact the performance of light detection and ranging systems and cause the AI subsystem to receive unreliable input for object classification [166]. Developing AI algorithms resilient in unpredictable operating conditions and robust in urban environments is essential to support IoV applications. Furthermore, AI algorithms are computationally intensive and rely on powerful computing resources with high energy consumption, such as graphics processing units (GPUs). Although there are hardware improvements that improve the performance of GPUs, such as field-programmable gate arrays, the development of high-performance hardware resources with low energy usage for large-scale commercial AI applications are required in IoV [167].

VII. Conclusion

Addressing interoperability challenges in IoV is crucial for assuring sustainable services and integrating heterogeneous entities that can support these services and applications. In this paper, we investigate interoperability challenges in IoV and present a detailed classification of limitations to interoperability. We provide a comprehensive survey of proposed methods to address IoV interoperability and present some open problems to consider for future work to secure a strategic advantage in the smart city ecosystem. We posit that IoV interoperability requires high intelligence techniques, adaptable network design, and a suitable balance between security and privacy. Addressing these challenges will facilitate the realization of an integrated ecosystem that enhances seamless, real-time communication of entities in the network to achieve the promising vision of IoV.

References

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

[2] 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.

[3] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin, and X. Liu, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.

[4] IEEE, "Ieee standard glossary of software engineering terminology (std. 610.12-1990)," 1990.

[5] S. K. Datta, J. Haerri, C. Bonnet, and R. F. Da Costa, "Vehicles as connected resources: Opportunities and challenges for the future," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 26–35, 2017.

[6] J. Toutouh and E. Alba, "Light commodity devices for building vehicular ad hoc networks: An experimental study," *Ad Hoc Networks*, vol. 37, pp. 499–511, 2016.

[7] M. Noura, M. Atiquzzaman, and M. Gaedke, "Interoperability in internet of things: Taxonomies and open challenges," *Mobile Networks and Applications*, vol. 24, no. 3, pp. 796–809, 2019.

[8] E. Lee, Y.-D. Seo, S.-R. Oh, and Y.-G. Kim, "A survey on standards for interoperability and security in the internet of things," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 2, 2021.

[9] H. Rahman and M. I. Hussain, "A comprehensive survey on semantic interoperability for internet of things: State-of-the-art and research challenges," *Transactions on Emerging Telecommunications Technologies*, vol. 31, no. 12, p. e3902, 2020.

[10] V. R. Konduru and M. R. Bharamagoudra, "Challenges and solutions of interoperability on iot: How far have we come in resolving the iot interoperability issues," in *2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon)*. IEEE, 2017.

[11] T. Perumal, C. Y. Leong, K. Samsudin, S. Mansor *et al.*, "Interoperability among heterogeneous systems in smart home environment," in *Web-Based Information Technologies and Distributed Systems*. Springer, 2010, pp. 141–157.

[12] K.-D. Moon, Y.-H. Lee, C.-E. Lee, and Y.-S. Son, "Design of a universal middleware bridge for device interoperability in heterogeneous home network middleware," *IEEE Transactions on Consumer Electronics*, vol. 51, no. 1, pp. 314–318, 2005.

[13] S. H. Park, M. J. Lee, and S. J. Kang, "Multimedia room bridge adapter for seamless interoperability between heterogeneous home network devices," in *Proceedings of the 15th ACM Mardi Gras conference*, 2008, pp. 1–9.

[14] H. Park, J.-H. Park, and N. Kim, "A framework for interoperability of heterogeneous devices in ubiquitous home," in *2010 Second International Conference on Advances in Future Internet*. IEEE, 2010.

[15] A. Zeid, S. Sundaram, M. Moghaddam, S. Kamarthi, and T. Marion, "Interoperability in smart manufacturing: Research challenges," *Machines*, vol. 7, no. 2, p. 21, 2019.

[16] S. M. Hussain, K. M. Yusof, and S. A. Hussain, "Interoperability in connected vehicles–a review," 2019.

[17] S. M. Hussain, K. M. Yosof, and S. A. Hussain, "Interoperability issues in internet of vehicles-a survey," in *2018 3rd International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 2018, pp. 257–262.

[18] S. Pantsar-Syväniemi, A. Purhonen, E. Ovaska, J. Kuusijärvi, and A. Evesti, "Situation-based and self-adaptive applications for the smart environment," *Journal of Ambient Intelligence and Smart Environments*, vol. 4, no. 6, pp. 491–516, 2012.

[19] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, "Internet of vehicles: architecture, protocols, and security," *IEEE internet of things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.

[20] A. Durmusoglu and Z. D. U. Durmusoglu, "Traffic control system technologies for road vehicles: A patent analysis," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 31–41, 2020.

[21] M. N. Sadiku, M. Tembely, and S. M. Musa, "Internet of vehicles: An introduction," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 8, no. 1, p. 11, 2018.

[22] K. Liu, X. Xu, M. Chen, B. Liu, L. Wu, and V. C. Lee, "A hierarchical architecture for the future internet of vehicles," *IEEE Communications Magazine*, vol. 57, no. 7, pp. 41–47, 2019.

[23] Y. Liu and G. Zhou, "Key technologies and applications of internet of things," in *2012 Fifth International Conference on Intelligent Computation Technology and Automation*. IEEE, 2012, pp. 197–200.

[24] M. Bilal, "A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3d printers," *arXiv preprint arXiv:1708.04560*, 2017.

[25] G. Bloom, B. Alsulami, E. Nwafor, and I. C. Bertolotti, "Design patterns for the industrial internet of things," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*. IEEE, 2018, pp. 1–10.

[26] M. Elkhodr, S. Shahrestani, and H. Cheung, "The internet of things: New interoperability, management and security challenges," *arXiv preprint arXiv:1604.04824*, 2016.

[27] R. Popescu-Zeletin, I. Radusch, and M. A. Rigani, *Vehicular-2-X communication: state-of-the-art and research in mobile vehicular ad hoc networks*. Springer Science & Business Media, 2010.

[28] A. Jafari, S. Al-Khayatt, and A. Dogman, "Performance evaluation of ieee 802.11 p for vehicular communication networks," in *2012 8th international symposium on communication systems, networks & digital signal processing (CSNDSP)*. IEEE, 2012, pp. 1–5.

[29] 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, 2018.

[30] L. Qi, "Research on intelligent transportation system technologies and applications," in *2008 Workshop on Power Electronics and Intelligent Transportation System*. IEEE, 2008, pp. 529–531.

[31] X. Wang, M. Chen, M. Zhu, and P. Tremont, "Development of a kinematic-based forward collision warning algorithm using an advanced driving simulator," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 9, pp. 2583–2591, 2016.

[32] R. K. Satzoda and M. M. Trivedi, "Multipart vehicle detection using symmetry-derived analysis and active learning," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 926–937, 2015.

[33] X. Xiong, L. Chen, and J. Liang, "A new framework of vehicle collision prediction by combining svm and hmm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 3, pp. 699–710, 2017.

[34] R. S. Tomar, S. Verma, R. Kushwah, and G. S. Tomar, "Collision avoidance warning for safe lane change," in *2013 International Conference on Communication Systems and Network Technologies*. IEEE, 2013, pp. 385–389.

[35] C.-C. Wang, S.-S. Huang, and L.-C. Fu, "Driver assistance system for lane detection and vehicle recognition with night vision," in *2005 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2005, pp. 3530–3535.

[36] V. C. Magana, X. G. Paneda, A. G. Tuero, L. Pozueco, R. Garcia, D. Melendi, and A. Rionda, "A method for making a fair evaluation of driving styles in different scenarios with recommendations for their improvement," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 136–148, 2018.

[37] N. Alsaffar, H. Ali, and W. Elmedany, "Smart transportation system: a review of security and privacy issues," in *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*. IEEE, 2018, pp. 1–4.

[38] M. A. Javed, E. Ben Hamida, and W. Znaidi, "Security in intelligent transport systems for smart cities: From theory to practice," *Sensors*, vol. 16, no. 6, p. 879, 2016.

[39] A. Lamssaggad, N. Benamar, A. S. Hafid, and M. Msahli, "A survey on the current security landscape of intelligent transportation systems," *IEEE Access*, vol. 9, pp. 9180–9208, 2021.

[40] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, "Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2017.

[41] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *International Conference on Ad hoc networks*. Springer, 2010, pp. 1–16.

[42] S. Abdelhamid, H. S. Hassanein, and G. Takahara, "Vehicle as a resource (vaar)," *IEEE Network*, vol. 29, no. 1, pp. 12–17, 2015.

[43] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, J. Wang *et al.*, "Vehicle-to-vehicle communications: readiness of v2v technology for application." United States. National Highway Traffic Safety Administration, Tech. Rep., 2014.

[44] C. Dai, X. Liu, W. Chen, and C.-F. Lai, "A low-latency object detection algorithm for the edge devices of iov systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 10, pp. 11 169–11 178, 2020.

[45] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of vehicle-to-grid on the distribution grid," *Electric Power Systems Research*, vol. 81, no. 1, pp. 185–192, 2011.

[46] S.-I. Sou and O. K. Tonguz, "Enhancing vanet connectivity through roadside units on highways," *IEEE transactions on vehicular technology*, vol. 60, no. 8, pp. 3586–3602, 2011.

[47] J. Cheng, G. Yuan, M. Zhou, S. Gao, C. Liu, H. Duan, and Q. Zeng, "Accessibility analysis and modeling for iov in an urban scene," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4246–4256, 2020.

[48] J. Zhang and K. B. Letaief, "Mobile edge intelligence and computing for the internet of vehicles," *Proceedings of the IEEE*, vol. 108, no. 2, pp. 246–261, 2019.

[49] S. Sun, J. Bi, M. Guillen, and A. M. Pérez-Marín, "Assessing driving risk using internet of vehicles data: An analysis based on generalized linear models," *Sensors*, vol. 20, no. 9, p. 2712, 2020.

[50] L. Atzori, A. Floris, R. Girau, M. Nitti, and G. Pau, "Towards the implementation of the social internet of vehicles," *Computer Networks*, vol. 147, pp. 132–145, 2018.

[51] D. Furelos Blanco, A. Bucchiarone, and A. Jonsson, "Carpool: collective adaptation using concurrent planning," in *AAMAS 2018. 17th International Conference on Autonomous Agents and Multiagent Systems; 2018 Jul 10-15; Stockholm, Sweden.[Richland]: IFAAMAS; 2018.* International Foundation for Autonomous Agents and Multiagent Systems (IFAAMAS), 2018.

[52] A. Al-Fuqaha, V. Kwigizile, J. Oh *et al.*, "Vehicle-to-device (v2d) communications: readiness of the technology and potential applications for people with disability," Western Michigan University, Tech. Rep., 2018.

[53] J. J. Anaya, P. Merdrignac, O. Shagdar, F. Nashashibi, and J. E. Naranjo, "Vehicle to pedestrian communications for protection of vulnerable road users," in *2014 IEEE Intelligent Vehicles Symposium Proceedings*. IEEE, 2014, pp. 1037–1042.

[54] D. O. Pop, A. Rogozan, F. Nashashibi, and A. Bensrhair, "Pedestrian recognition using cross-modality learning in convolutional neural networks," *IEEE Intelligent Transportation Systems Magazine*, vol. 13, no. 1, pp. 210–224, 2020.

[55] C. C. Secretariat, "Civil contingencies act 2004: a short guide (revised)," *London: Cabinet Office*, 2004.

[56] S. K. Datta, C. Bonnet, and J. Haerri, "Fog computing architecture to enable consumer centric internet of things services," in *2015 International Symposium on Consumer Electronics (ISCE)*. IEEE, 2015, pp. 1–2.

[57] T. Zugno, M. Drago, M. Giordani, M. Polese, and M. Zorzi, "Toward standardization of millimeter-wave vehicle-to-vehicle networks: Open challenges and performance evaluation," *IEEE Communications Magazine*, vol. 58, no. 9, pp. 79–85, 2020.

[58] A. Bazzi, B. M. Masini, A. Zanella, and I. Thibault, "On the performance of ieee 802.11 p and lte-v2v for the cooperative awareness of connected vehicles," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 419–10 432, 2017.

[59] S. Zeadally, M. A. Javed, and E. B. Hamida, "Vehicular communications for its: standardization and challenges," *IEEE Communications Standards Magazine*, vol. 4, no. 1, pp. 11–17, 2020.

[60] A. Ahamed and H. Vakilzadian, "Issues and challenges in vanet routing protocols," in *2018 IEEE international conference on electro/information technology (EIT)*. IEEE, 2018, pp. 0723–0728.

[61] T. Kayarga and S. A. Kumar, "A study on various technologies to solve the routing problem in internet of vehicles (iov)," *Wireless Personal Communications*, pp. 1–29, 2021.

[62] R. Poorzare and A. C. Augé, "Challenges on the way of implementing tcp over 5g networks," *IEEE access*, vol. 8, pp. 176 393–176 415, 2020.

[63] T. Berners-Lee, J. Hendler, and O. Lassila, "The semantic web," *Scientific american*, vol. 284, no. 5, pp. 34–43, 2001.

[64] Y.-B. Lin, D.-J. Deng, I. You, and C.-C. Lin, *IoT as a Service: Third International Conference, IoTaaS 2017, Taichung, Taiwan, September 20–22, 2017, Proceedings*. Springer, 2018, vol. 246.

[65] G. Wohlgenannt, A. Weichselbraun, A. Scharl, and M. Sabou, "Dynamic integration of multiple evidence sources for ontology learning," *Journal of Information and Data Management*, vol. 3, pp. 243–254, 2012.

[66] N. Kolbe, S. Kubler, J. Robert, Y. Le Traon, and A. Zaslavsky, "Towards semantic interoperability in an open iot ecosystem for connected vehicle services," in *2017 Global Internet of Things Summit (GIoTS)*. IEEE, 2017, pp. 1–5.

[67] L. Zhao, R. Ichise, S. Mita, and Y. Sasaki, "Core ontologies for safe autonomous driving." in *International Semantic Web Conference (Posters & Demos)*, 2015.

[68] S. Kannan, A. Thangavelu, and R. Kalivaradhan, "An intelligent driver assistance system (i-das) for vehicle safety modelling using ontology approach," *International Journal of UbiComp*, vol. 1, no. 3, pp. 15–29, 2010.

[69] B. Klotz, S. K. Datta, D. Wilms, R. Troncy, and C. Bonnet, "A car as a semantic web thing: Motivation and demonstration," in *2018 Global Internet of Things Summit (GIoTS)*. IEEE, 2018, pp. 1–6.

[70] J. Barrachina, P. Garrido, M. Fogue, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "Caova: A car accident ontology for vanets," in *2012 IEEE wireless communications and networking conference (WCNC)*. Ieee, 2012, pp. 1864–1869.

[71] M. Burgess and R. Hale-Evans, "The gnu c programming tutorial," 2002.

[72] K. Ibrahim and M. C. Weigle, "Cascade: Cluster-based accurate syntactic compression of aggregated data in vanets," in *2008 IEEE Globecom Workshops*. IEEE, 2008, pp. 1–10.

[73] R. ElHakim, A. Elqadi, M. Torky, M. Zayed, I. Farag, and M. Agamawi, "Let's do-automotive platform for interoperability," in *2021 4th International Conference on Information and Computer Technologies (ICICT)*. IEEE, 2021, pp. 294–299.

[74] S. Soursos, I. P. Žarko, P. Zwickl, I. Gojmerac, G. Bianchi, and G. Carrozzo, "Towards the cross-domain interoperability of iot platforms," in *2016 European conference on networks and communications (EuCNC)*. IEEE, 2016, pp. 398–402.

[75] S. Soursos, I. P. Zarko, and I. Book, "Symbiote: Symbiosis of smart objects across iot environments," in *Digitising the Industry—Internet of Things Connecting the Physical, Digital and Virtual Worlds*. River Publishers, 2016, pp. 303–307.

[76] "Discipline – application interoperability," accessed: 02-01-2019. [Online]. Available: https://oa.mo.gov/sites/default/files/DSP-ApplicationInteroperability031004.pdf

[77] X. Wang, Z. Ning, M. Zhou, X. Hu, L. Wang, Y. Zhang, F. R. Yu, and B. Hu, "Privacy-preserving content dissemination for vehicular social networks: Challenges and solutions," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1314–1345, 2018.

[78] C. Lai, R. Lu, D. Zheng, and X. Shen, "Security and privacy challenges in 5g-enabled vehicular networks," *IEEE Network*, vol. 34, no. 2, pp. 37–45, 2020.

[79] A. S. Chekkouri, A. Ezzouhairi, and S. Pierre, "A new integrated vanet-lte-a architecture for enhanced mobility in small cells hetnet using dynamic gateway and traffic forwarding," *Computer Networks*, vol. 140, pp. 15–27, 2018.

[80] D.-Y. Kim, M. Jung, and S. Kim, "An internet of vehicles (iov) access gateway design considering the efficiency of the in-vehicle ethernet backbone," *Sensors*, vol. 21, no. 1, p. 98, 2021.

[81] X. Wang, Y. Weng, and H. Gao, "A low-latency and energy-efficient multimetric routing protocol based on network connectivity in vanet communication," *IEEE Transactions on Green Communications and Networking*, 2021.

[82] I. Achour, T. Bejaoui, A. Busson, and S. Tabbane, "Sead: A simple and efficient adaptive data dissemination protocol in vehicular ad-hoc networks," *Wireless Networks*, vol. 22, no. 5, pp. 1673–1683, 2016.

[83] S. Nam, H. Kim, and S.-G. Min, "Simplified stream reservation protocol over software-defined networks for in-vehicle time-sensitive networking," *IEEE Access*, vol. 9, pp. 84 700–84 711, 2021.

[84] R. Gasmi, M. Aliouat, and H. Seba, "A stable link based zone routing protocol (sl-zrp) for internet of vehicles environment," *Wireless Personal Communications*, vol. 112, no. 2, pp. 1045–1060, 2020.

[85] K. Afzal, R. Tariq, F. Aadil, Z. Iqbal, N. Ali, and M. Sajid, "An optimized and efficient routing protocol application for iov," *Mathematical Problems in Engineering*, vol. 2021, 2021.

[86] K. Mershad, "Surfer: A secure sdn-based routing protocol for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 9, 2020.

[87] N. Omar, N. Yaakob, Z. Husin, and M. Elshaikh, "Design and development of greedlea routing protocol for internet of vehicle (iov)," in *IOP Conference Series: Materials Science and Engineering*, vol. 767, no. 1. IOP Publishing, 2020, p. 012034.

[88] R. Attia, A. Hassaan, and R. Rizk, "Advanced greedy hybrid bio-inspired routing protocol to improve iov," *IEEE Access*, vol. 9, pp. 131 260–131 272, 2021.

[89] C.-W. Lee, M. C. Chen, and Y. S. Sun, "Protocol and architecture supports for network mobility with qos-handover for high-velocity vehicles," *Wireless Networks*, vol. 19, no. 5, pp. 811–830, 2013.

[90] H. Nashaat, "Qos-aware cross layer handover scheme for high-speed vehicles," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 12, no. 1, pp. 135–158, 2018.

[91] S. H. Ahmed, H. Kang, and D. Kim, "Vehicular delay tolerant network (vdtn): Routing perspectives," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)*. IEEE, 2015, pp. 898–903.

[92] A. S. Vieira, J. Goncalves Filho, J. Celestino, and A. Patel, "Vdtn-tod: routing protocol vanet/dtn based on trend of delivery," in *Advanced International Conference on Telecommunications, AICT*. Citeseer, 2013.

[93] N. I. Er, K. D. Singh, and J.-M. Bonnin, "Dc4led: A hierarchical vdtn routing for data collection in smart cities," in *2019 16th IEEE annual consumer communications & networking conference (CCNC)*. IEEE, 2019, pp. 1–4.

[94] X. Guo, Y. Chen, L. Cao, D. Zhang, and Y. Jiang, "A smart forwarding scheme for the interest packet in vndn," in *2019 2nd International Conference on Hot Information-Centric Networking (HotICN)*. IEEE, 2019, pp. 7–12.

[95] Z. Yan, S. Zeadally, and Y.-J. Park, "A novel vehicular information network architecture based on named data networking (ndn)," *IEEE internet of things journal*, vol. 1, no. 6, pp. 525–532, 2014.

[96] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, and M. Gerla, "Conet: Controlled data packets propagation in vehicular named data networks," in *2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2016, pp. 620–625.

[97] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-defined networking for rsu clouds in support of the internet of vehicles," *IEEE Internet of Things journal*, vol. 2, no. 2, pp. 133–144, 2014.

[98] S. Correia, A. Boukerche, and R. I. Meneguette, "An architecture for hierarchical software-defined vehicular networks," *IEEE Communications Magazine*, vol. 55, no. 7, pp. 80–86, 2017.

[99] S. Smaldone, L. Han, P. Shankar, and L. Iftode, "Roadspeak: enabling voice chat on roadways using vehicular social networks," in *Proceedings of the 1st Workshop on Social Network Systems*, 2008, pp. 43–48.

[100] X. Hu, V. C. Leung, K. G. Li, E. Kong, H. Zhang, N. S. Surendrakumar, and P. TalebiFard, "Social drive: a crowdsourcing-based vehicular social networking system for green transportation," in *Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications*, 2013, pp. 85–92.

[101] K. M. Alam, M. Saini, and A. El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE access*, vol. 3, pp. 343–357, 2015.

[102] X. He, Z. Ren, C. Shi, and J. Fang, "A novel load balancing strategy of software-defined cloud/fog networking in the internet of vehicles," *China Communications*, vol. 13, no. Supplement2, pp. 140–149, 2016.

[103] Y. Zhang, C. Li, T. H. Luan, Y. Fu, W. Shi, and L. Zhu, "A mobility-aware vehicular caching scheme in content centric networks: Model and optimization," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 4, pp. 3100–3112, 2019.

[104] Z. Ning, K. Zhang, X. Wang, L. Guo, X. Hu, J. Huang, B. Hu, and R. Y. Kwok, "Intelligent edge computing in internet of vehicles: a joint computation offloading and caching solution," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 4, pp. 2212–2225, 2020.

[105] S. Chun, S. Shin, S. Seo, S. Eom, J. Jung, and K.-H. Lee, "A pub/sub-based fog computing architecture for internet-of-vehicles," in *2016 IEEE international conference on cloud computing technology and science (CloudCom)*. IEEE, 2016, pp. 90–93.

[106] M. Liu, Y. Teng, F. R. Yu, V. C. Leung, and M. Song, "Deep reinforcement learning based performance optimization in blockchain-enabled internet of vehicle," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.

[107] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, "A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2019.

[108] A. Hbaieb, J. Rezgui, and L. Chaari, "Pedestrian detection for autonomous driving within cooperative communication system," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 2019, pp. 1–6.

[109] A. Hbaieb, O. B. Rhaiem, and L. Chaari, "In-car gateway architecture for intra and inter-vehicular networks," in *2018 14th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2018, pp. 1489–1494.

[110] I. Jabri, T. Mekki, A. Rachedi, and M. B. Jemaa, "Vehicular fog gateways selection on the internet of vehicles: A fuzzy logic with ant colony optimization based approach," *Ad Hoc Networks*, vol. 91, p. 101879, 2019.

[111] D. Abada, A. Massaq, A. Boulouz, and M. Ben Salah, "An adaptive vehicular relay and gateway selection scheme for connecting vanets to internet via 4g lte cellular network," in *Emerging technologies for connected internet of vehicles and intelligent transportation system networks*. Springer, 2020, pp. 149–163.

[112] X. Duan, X. Wang, Y. Liu, and K. Zheng, "Sdn enabled dual cluster head selection and adaptive clustering in 5g-vanet," in *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall)*. IEEE, 2016, pp. 1–5.

[113] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*. IEEE, 1999.

[114] D. B. Johnson, D. A. Maltz, J. Broch *et al.*, "Dsr: The dynamic source routing protocol for multi-hop wireless ad hoc networks," *Ad hoc networking*, vol. 5, no. 1, pp. 139–172, 2001.

[115] G. He, "Destination-sequenced distance vector (dsdv) protocol," *Networking Laboratory, Helsinki University of Technology*, vol. 135, 2002.

[116] S. Lu, L. Li, K.-Y. Lam, and L. Jia, "Saodv: a manet routing protocol that can withstand black hole attack," in *2009 international conference on computational intelligence and security*. IEEE, 2009, pp. 421–425.

[117] D. Zhang, C. Gong, T. Zhang, J. Zhang, and M. Piao, "A new algorithm of clustering aodv based on edge computing strategy in iov," *Wireless Networks*, vol. 27, no. 4, pp. 2891–2908, 2021.

[118] T. Gerhard, T. Kobzan, I. Blöcher, and M. Hendel, "Software-defined flow reservation: Configuring ieee 802.1 q time-sensitive networks by

the use of software-defined networking," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 216–223.

[119] D. Bujosa, I. Álvarez, D. Čavka, and J. Proenza, "Analysing termination and consistency in the avb's stream reservation protocol," in *2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 1309–1312.

[120] A. Balasubramanian, R. Mahajan, A. Venkataramani, B. N. Levine, and J. Zahorjan, "Interactive wifi connectivity for moving vehicles," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 4, pp. 427–438, 2008.

[121] C. E. Perkins, "Mobile ip," *IEEE communications Magazine*, vol. 35, no. 5, pp. 84–99, 1997.

[122] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert, "Network mobility (nemo) basic support protocol," 2005.

[123] S. Imadali, V. Veque, and A. Petrescu, "Analyzing dynamic ipv6 address auto-configuration techniques for group ip-based vehicular communications," in *39th Annual IEEE Conference on Local Computer Networks Workshops*. IEEE, 2014, pp. 722–729.

[124] S. Cespedes, X. Shen, and C. Lazo, "Ip mobility management for vehicular communication networks: challenges and solutions," *IEEE Communications Magazine*, vol. 49, no. 5, pp. 187–194, 2011.

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

[126] J. Gonçalves Filho, A. Patel, B. L. A. Batista, and J. C. Júnior, "A systematic technical survey of dtn and vdtn routing protocols," *Computer Standards & Interfaces*, vol. 48, pp. 139–159, 2016.

[127] J. Härri, C. Bonnet, and F. Filali, "Kinetic mobility management applied to vehicular ad hoc network protocols," *Computer Communications*, vol. 31, no. 12, pp. 2907–2924, 2008.

[128] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *ACM SIGMOBILE mobile computing and communications review*, vol. 7, no. 3, pp. 19–20, 2003.

[129] A. Vahdat, D. Becker *et al.*, "Epidemic routing for partially connected ad hoc networks," 2000.

[130] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, 2005, pp. 252–259.

[131] J. Wang, R. Wakikawa, and L. Zhang, "Dmnd: Collecting data from mobiles using named data," in *2010 IEEE Vehicular Networking Conference*. IEEE, 2010, pp. 49–56.

[132] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[133] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," *ACM SIGCOMM computer communication review*, vol. 38, no. 2, pp. 69–74, 2008.

[134] D. F. Macedo, D. Guedes, L. F. Vieira, M. A. Vieira, and M. Nogueira, "Programmable networks—from software-defined radio to software-defined networking," *IEEE communications surveys & tutorials*, vol. 17, no. 2, pp. 1102–1125, 2015.

[135] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.

[136] C. Jiacheng, Z. Haibo, Z. Ning, Y. Peng, G. Lin, and S. X. Sherman, "Software defined internet of vehicles: Architecture, challenges and solutions," *Journal of communications and information networks*, vol. 1, no. 1, pp. 14–26, 2016.

[137] M. Nitti, R. Girau, A. Floris, and L. Atzori, "On adding the social dimension to the internet of vehicles: Friendship and middleware," in *2014 IEEE international black sea conference on communications and networking (BlackSeaCom)*. IEEE, 2014, pp. 134–138.

[138] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (siot)–when social networks meet the internet of things: Concept, architecture and network characterization," *Computer networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[139] R. Silva and R. Iqbal, "Ethical implications of social internet of vehicles systems," *IEEE Internet of Things Journal*, vol. 6, pp. 517–531, 2018.

[140] T. A. Butt, R. Iqbal, S. C. Shah, and T. Umar, "Social internet of vehicles: Architecture and enabling technologies," *Computers & Electrical Engineering*, vol. 69, pp. 68–84, 2018.

[141] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the internet of things," in *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*, 2012, pp. 13–16.

[142] H. Le, K. Boussetta, and N. Achir, "A unified and semantic data model for fog computing," in *2020 Global Information Infrastructure and Networking Symposium (GIIS)*. IEEE, 2020, pp. 1–6.

[143] L. Silva, N. Magaia, B. Sousa, A. Kobusińska, A. Casimiro, C. X. Mavromoustakis, G. Mastorakis, and V. H. C. De Albuquerque, "Computing paradigms in emerging vehicular environments: a review," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 3, pp. 491–511, 2021.

[144] A. Hussain, M. Iqbal, S. Sarwar, M. Safyan, Z. ul Qayyum, H. Gao, and X. Wang, "Servicing delay sensitive pervasive communication through adaptable width channelization for supporting mobile edge computing," *Computer Communications*, vol. 162, pp. 152–159, 2020.

[145] C. Wang, C. Liang, F. R. Yu, Q. Chen, and L. Tang, "Computation offloading and resource allocation in wireless cellular networks with mobile edge computing," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 4924–4938, 2017.

[146] H. Peng and X. Shen, "Deep reinforcement learning based resource management for multi-access edge computing in vehicular networks," *IEEE Transactions on Network Science and Engineering*, vol. 7, no. 4, pp. 2416–2428, 2020.

[147] Y. Liu, H. Yu, S. Xie, and Y. Zhang, "Deep reinforcement learning for offloading and resource allocation in vehicle edge computing and networks," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11 158–11 168, 2019.

[148] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[149] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications," in *Proceedings First International Conference on Peer-to-Peer Computing*. IEEE, 2001, pp. 101–102.

[150] M. Belotti, N. Božić, G. Pujolle, and S. Secci, "A vademecum on blockchain technologies: When, which, and how," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3796–3838, 2019.

[151] S. Goyal, "Centralized vs decentralized vs distributed," 2015. [Online]. Available: https://medium.com/delta-exchange/centralized-vs-decentralized-vs-distributed-41d92d463868

[152] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: Distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, 2018.

[153] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K.-Y. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4157–4185, 2020.

[154] G. Tripathi, M. A. Ahad, and M. Sathiyanarayanan, "The role of blockchain in internet of vehicles (iov): issues, challenges and opportunities," in *2019 International Conference on contemporary Computing and Informatics (IC3I)*. IEEE, 2019, pp. 26–31.

[155] S. R. Pokhrel and J. Choi, "Federated learning with blockchain for autonomous vehicles: Analysis and design challenges," *IEEE Transactions on Communications*, vol. 68, no. 8, pp. 4734–4746, 2020.

[156] K. N. Qureshi, S. Din, G. Jeon, and F. Piccialli, "Internet of vehicles: Key technologies, network model, solutions and challenges with future aspects," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 3, pp. 1777–1786, 2020.

[157] K. Smida, H. Tounsi, M. Frikha, and Y.-Q. Song, "Software defined internet of vehicles: a survey from qos and scalability perspectives," in *2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC)*. IEEE, 2019, pp. 1349–1354.

[158] C. R. Storck and F. Duarte-Figueiredo, "A survey of 5g technology evolution, standards, and infrastructure associated with vehicle-to-everything communications by internet of vehicles," *IEEE Access*, vol. 8, pp. 117 593–117 614, 2020.

[159] X. Wang, L. Kong, F. Kong, F. Qiu, M. Xia, S. Arnon, and G. Chen, "Millimeter wave communication: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1616–1653, 2018.

[160] R. He, C. Schneider, B. Ai, G. Wang, Z. Zhong, D. A. Dupleich, R. S. Thomae, M. Boban, J. Luo, and Y. Zhang, "Propagation channels of 5g millimeter-wave vehicle-to-vehicle communications: Recent advances and future challenges," *IEEE vehicular technology magazine*, vol. 15, no. 1, pp. 16–26, 2019.

[161] C.-X. Wang, J. Huang, H. Wang, X. Gao, X. You, and Y. Hao, "6g wireless channel measurements and models: Trends and challenges," *IEEE Vehicular Technology Magazine*, vol. 15, no. 4, pp. 22–32, 2020.

[162] A. Bröring, A. Ziller, V. Charpenay, A. S. Thuluva, D. Anicic, S. Schmid, A. Zappa, M. P. Linares, L. Mikkelsen, and C. Seidel, "The big iot api-semantically enabling iot interoperability," *IEEE Pervasive Computing*, vol. 17, no. 4, pp. 41–51, 2018.

[163] F. Carrez, T. Elsaleh, D. Gómez, L. Sánchez, J. Lanza, and P. Grace, "A reference architecture for federating iot infrastructures supporting semantic interoperability," in *2017 European Conference on Networks and Communications (EuCNC)*. IEEE, 2017, pp. 1–6.

[164] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11 815–11 829, 2020.

[165] R. Iqbal, T. A. Butt, M. Afzaal, and K. Salah, "Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions," *International Journal of Distributed Sensor Networks*, vol. 15, no. 1, p. 1550147719825820, 2019.

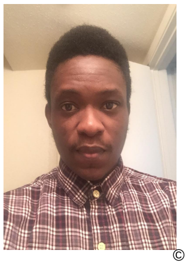
[166] P. Radecki, M. Campbell, and K. Matzen, "All weather perception: Joint data association, tracking, and classification for autonomous ground vehicles," *arXiv preprint arXiv:1605.02196*, 2016.

[167] Y. Ma, Z. Wang, H. Yang, and L. Yang, "Artificial intelligence applications in the development of autonomous vehicles: a survey," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 2, pp. 315–329, 2020.

Paul Agbaje is a Ph.D. student in the Computer Science and Engineering Department at The University of Texas at Arlington. He obtained his bachelor's degree in Electrical and Electronics Engineering from the University of Ilorin, Nigeria. His current research focuses on interoperability issues in internet-of-vehicles and cyber-physical system security.

Afia Anjum is a Ph.D. student in the Computer Science and Engineering Department at The University of Texas at Arlington. She is currently pursuing her research in the Cyber-Physical System Security Laboratory. Her research mainly focuses on the security and trustworthiness of the Internet of Things, Internet of Vehicles, autonomous vehicles, embedded systems, and emerging networks.

Arkajyoti Mitra is a Ph.D. student in the Computer Science and Engineering Department at The University of Texas at Arlington. He received his master's degree in Computer Science from The Indian Institute of Technology, Dhanbad, and his bachelor's degree in Computer Science from Kalyani Government Engineering College in India. His research focus includes sensor-based perception systems, detecting vulnerabilities in vehicular architecture in autonomous vehicles, and computer vision.



Emmanuel Oseghale is a Ph.D. student in the Computer Science and Engineering department at The University of Texas at Arlington. He works at the Cyber-Physical System Security Laboratory. His research interest includes investigating security issues in vehicular network, trust framework for vehicle node communication, and real-time distributed embedded System.

Gedare Bloom (SM'19) received his Ph.D. in computer science from The George Washington University in 2013. He joined the University of Colorado Colorado Springs as Assistant Professor of Computer Science in 2019. He was Assistant Professor of Computer Science at Howard University from 2015-2019. His research expertise is computer system security with emphasis on real-time embedded systems. He is an associate editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY.

Habeeb Olufowobi received his Ph.D. in computer science from Howard University in 2019. He joined University of Texas at Arlington as Assistant Professor of Computer Science and Engineering in 2020. He joined the University of Texas at Arlington as an Assistant Professor of Computer Science and Engineering in 2020. His research focuses on embedded systems and security and privacy challenges in emerging network technologies for connected autonomous vehicles, the Internet of Vehicles (IoV) in a smart city ecosystem, and vehicular cloud network.