Article citation info:
Alhabib MH, Ali QI. Internet of autonomous vehicles communication infrastructure: a short review. Diagnostyka. 2023;24(3):2023302.
https://doi.org/10.29354/diag/168310.

DIAGNOSTYKA, 2023, Vol. 24, No. 3

e-ISSN 2449-5220
DOI: 10.29354/diag/168310

INTERNET OF AUTONOMOUS VEHICLES COMMUNICATION INFRASTRUCTURE: A SHORT REVIEW

Mustafa Haitham ALHABIB [*], **Qutaiba Ibrahim ALI**

Computer Engineering Department, University of Mosul, Iraq
[*] Corresponding author, e-mail: mustafa.20enp4@student.uomosul.edu.iq

Abstract

Recent years have witnessed increased attention towards vehicular communications as a part of an overall modernization trend towards the emergence of a reliable, less human-dependent, and more efficient Intelligent Transportation System (ITS) conjugated with the rapid growth of smart cities. ITS imposes better safety and security through the employment of Autonomous Vehicles (AV) to reduce the possibility of accidents caused due to human intervention. The application of autonomous vehicles to the traditional Vehicular Ad-hoc Networks (VANET) has paved the way for the development of a newer networking paradigm called the Internet of Autonomous Vehicles (IoAV). IoAV enjoys several advantages over VANET in terms of robustness, security, and scalability. However, due to the gradual transition from existing vehicles to autonomous ones, both types may be going to coexist together in the same environment. Therefore, a reliable, fast responsive, and flexible infrastructure is necessary to serve both kinds in such a hybrid setting until the transition to all AV is completed. In this context, this paper represents a concise review of the architecture of IoAV infrastructure, its communication modules, message dissemination, protocols and services that comprise the main body of the IoAV framework, in addition to further remarks and research challenges.

Keywords: ITS, IoAV, infrastructure, architecture, layers

List of Symbols/Acronyms

AODV - Ad hoc On-Demand Distance Vector
AV - Autonomous Vehicles
BSM - Basic Safety Message
DSDV - Destination Sequenced Distance Vector Routing
DSR - Dynamic Source Routing
DSRC - Dedicated Short Range Communications
ES - Edge Servers
FSR - Fisheye State Routing
IoAV - Internet of Autonomous Vehicles
IoT - Internet of Things
IoV - Internet of Vehicles
ITS - Intelligent Transportation System
LDWS - Lane Departure Warning System
LTW - Long-Term Evolution
MDV - Manually Driving Vehicles
OBU - Onboard Unit
OLSR - Optimized Link State Routing
QoS - Quality of Service
RSU - Road Side Units
SDN - Software Defined Networking
TORA - Temporally Ordered Routing Algorithm
V2I - Vehicle-to-Infrastructure
V2V - Vehicles-to-Vehicles
V2X - Vehicle-to-Everything
VANET - Vehicular Ad-hoc Networks
ZBP - Zone Routing Protocol

1. INTRODUCTION

The arrival of the term Internet of Things (IoT) by the end of the twentieth century has opened the door to a variety of technologies that contributed to the renovation of the human lifestyle as a part of the ongoing fourth Industrial Revolution (IR4.0) as depicted by some researchers [1]. Since mobility plays a major role in this modernization process, some of the IoT-based technologies were directed toward facilitating the task of traveling from one place to the other. This gave birth to the term Internet of Vehicles (IoV) as a subset technology of IoT [2], where vehicular communications take place among vehicles and other backbone units that serve as the infrastructure for the communicating units. A further step is to introduce the autonomous factor as a substitute for the human factor for better safety and improved economy, leading to the generation of another term, the Internet of Autonomous Vehicles (IoAV) [3]. Both IoV and IoAV paradigms contribute to the development of what is called the Intelligent Transportation System (ITS), an environment where Manually Driving Vehicles (MDV) and Autonomous Vehicles (AV) interacts with each other and with other units such are pedestrians, cyclist as well as the infrastructure to

Received 2023-02-08; Accepted 2023-06-14; Available online 2023-06-28

provide a more reliable level of connectivity for safety and non-safety applications [4].

The idea of autonomous driving roots back to the late nineties when vehicle manufacturers decided to adopt it as a response to the increased number of fatalities from traffic accidents, which, according to recent records, is mainly due to human misjudgement [5]. Later, this led to the invention of some semi-auto technologies that induce autonomy in certain cases like auto parking and cruise control [3]. Since MDVs rely heavily on human behaviour for action, transforming the vehicle for autonomy requires upgrading and arming it with a repertoire of capable sensors and communication interfaces to compensate for the absence of the human factor. Therefore, future AVs will be powerful platforms that collect useful data from their sensors, other AVs, and the infrastructure [3]. However, due to the heterogeneity of the involved components, relying solely on vehicles does not achieve the required level of connectivity as it does not guarantee the delivery of the time-sensitive safety-related messages within acceptable delay limits. Thus, using additional components as infrastructure is substantial to allow more flexibility to serve various components and to enhance the throughput, reliability, and safety of message dissemination [6, 7].

This requirement for a capable and flexible infrastructure calls for a composite design with multiple layers and various components, including Road Side Units (RSU), Micro Base Stations (MBS), and Edge Servers (ES) all being connected and with centralized cloud servers over wireless networks [8]. Though it was not previously common to use all of these elements together in one framework. The traditional form of vehicular communications was represented by Vehicular Ad-hoc Networks (VANET), a centralized network layout of connected vehicles using wireless routers and access points covering a certain geographical zone and exchanging useful information with a cloud server [9,10,11]. Despite its cloud-enabled computational and storage capabilities, VANETs suffer from a variety of pitfalls related to its cloud-dependent architecture, most notably the delay introduced due to its centralized nature which creates a bottleneck when interacting with the cloud processing and storage services, in addition to another compatibility, accuracy and reliability issues like the unattainability of cloud services in the absence of internet connection [8, 10]. Hence, over the past few years, VANET had progressed into IoV and is expected to continue its evolution to IoAV in the near future [2].

The goal of the paper in hand is to provide a short yet comprehensive digest on the communication infrastructure for IoAV that gives a first-glance review of related topics like layers and their roles, data transfer methods, protocols, services and applications, current challenges, and expected solutions. The rest of this paper is organized as follows: section 2 discusses some of the commonly presented infrastructures for IoAV, focusing on the layers, their roles and features. Section 3 addresses the communication models and data-sharing methods to be used among various nodes. The protocols that govern data transfer are briefly explained in section 4, the services and applications provided to the users by IoAV are given in section 5, the challenges opposing its execution in section 6. Finally, section 7 concludes the article.

2. IOAV INFRASTRUCTURE MODEL

An important design aspect of the IoAV infrastructure is the nature and distribution of its layers, a number of layered architectures have been proposed over the past few years with different roles and functionalities, one notable example is given by [3] where a three-layered architecture was presented for IoAV operation, which consisted of a physical layer, a virtual layer, and a management layer. These layers cooperate for providing the intended IoAV services while maintaining a real-time data exchange among its components. The physical layer focuses on communications, providing techniques for the realization of continuous and efficient connectivity for the upper layers. This is achieved by a variety of technologies, such as mmWave, cellular communications, and Dedicated Short Range Communications (DSRC), creating a suitable environment for the virtual layer, which provides the means for resource management and distribution following the rules issued by the management layer, comprising simple services into more complicated ones. This is where edge and fog computing are applied to give closer processing and storage capabilities to the physical layer, which improves flexibility and reduces the delay for delay-sensitive applications. The management layer sits at the top of the hierarchy and is responsible for preserving the heterogeneous nature of the network by issuing a suitable set of rules, monitoring the services provided, and supervising the cloud and edge servers while ensuring the security of the exchanged information.

Another salient study was presented by [8], proposing a VEC-enabled architecture as an answer to some of the challenges prominent in vehicular networks. Here too, the authors suggested a three-layered architecture as a vehicular framework, namely the smart vehicular layer, the edge cloud layer, and the cloud layer. The smart vehicular layer consists of a group of AVs closely connected by a wireless network and exchanging information at high data rates. The exchanged information is generated from a set of various sensors onboard the vehicle as well as cameras, Radar, Lidar, and other communication interfaces. The collected information is then uploaded to the edge cloud layer, which serves as an interface between the smart vehicular layer and the cloud layer, it provides inferior processing and storage capabilities to the cloud yet its decentralized nature and proximity to the vehicles allows for a better Quality of Service

(QoS) and reduced latency which is highly required for safety applications. Other more complex applications that require superior capabilities should be handled by the cloud layer, the cloud can also process the massive amounts of data produced by the vehicles (about 1 GB/s [3]) and accumulated by edge nodes, which are usually related to delay-insensitive services that do not require a real-time response. These applications can be put on hold by the cloud and executed later at very high speeds, even for complex applications. Despite its greater processing and storage abilities, the centralized nature of the cloud can cause transfer bottlenecks to appear between vehicles and remote servers, leading to larger delays that are undesirable for time-sensitive applications. Edge and fog computing are utilized to mitigate this issue by bringing the servers to the proximity of the vehicles while distributing them on multiple platforms, thus minimizing the possibility of bottlenecks and maintaining a cap on transmission latency for a variety of applications.

Though these layers are analogous to the layers presented by [3], references [8, 12] also introduce the concept of Software Defined Networking (SDN) as another solution to the delay of packet flow interrupts caused by the linkage between data and control planes. SDN attempts to disjoint the control plane from the data plane, resulting in more flexibility in network management, better conversant network decisions, and a global view to the controller, which gives a more effective network distribution and agile management acting independently from other networks. The complete layout of the architecture as portrayed by [8] is given in figure 1.

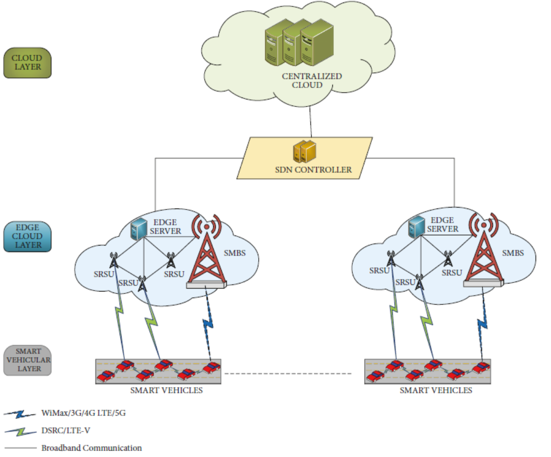

Fig. 1. Three-layer vehicular edge computing architecture

A similar layout was given by [13] with a 3-layer model consisting of edge smart devices, distributed fog, and the cloud layer. The smart devices, however, are not limited to vehicles but range to smartphones, street-embedded sensors, and cameras. Another suggested detail here is that the fog layer itself is classified into two sublayers where major fog nodes control the operation of minor ones. Also, fog nodes are to perform additional processing and caching tasks to control local and remote operations so that some of the applications will be diverted away from the cloud. The edge node is represented by both sensors and actuators in the model, while the fog node will be acting as its controller. Moreover, additional features can be added to the model as extra functionalities, performance improvements, or remedies against issues that may arise during operation or from outside (e.g. attacks). Reference [14] mentions a number of these technologies like Named Data Networking (NDN) to alleviate the time required for network address allocation, lightweight reputation mechanism (LRES) to boost the model's performance and effectiveness, and blockchain technology for ensuring privacy, security, and stability of data transactions.

Ultimately, the number of layers may vary for various studies, some architectures may propose up to five layers for more detailed tasks like in [2] which includes additional layers for acquisition, management, and processing. In this model, vehicular communications occur via the communication layer, management and network administration mechanisms (like edge computing) are performed at the control and management layer, while the processing layer is responsible for cloud operations, figure 2 outlines the tasks and details of each layer of the model as proposed by reference [2].

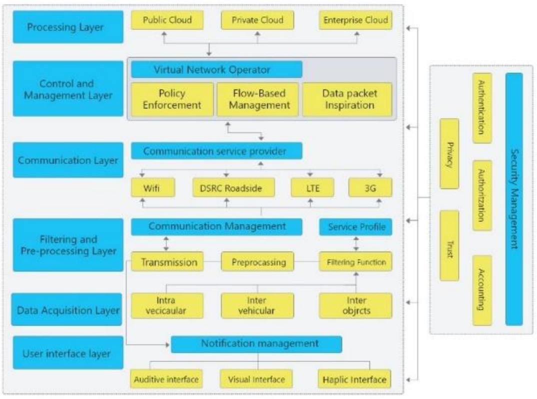

Fig. 2. The expanded Layered Architecture for IoAV

3. VEHICULAR COMMUNICATIONS FOR IOAV

Usually, when addressing the forms of vehicular communications, two main types stand out for discussion: Vehicles-to-Vehicles (V2V) and Vehicle-to-Infrastructure (V2I). However, other entities may also participate in the communications process such as RSU, pedestrians, and MBS, which are either utilized for data processing or for data relay to the required destination for providing the intended services to the network users. These vehicular communications can be divided into three main categories as follows [5, 8, 12].

3.1. Intravehicle Communication

Used to describe the transfer of information within one vehicle. As previously stated, the AV is equipped with a variety of sensors that provide a better perspective about its surrounding, all being connected to the vehicle's Onboard Unit (OBU), which oversees the transfer of the information regarding various services like object detection and traffic congestion. The OBU also acquires data from other AVs and the infrastructure and uses it to control the vehicle's actuators like motors and breaks. Traditionally, Intravehicle communications rely on wired networks for data exchange between the OBU and its peripherals. However, the adoption of wireless networks for this purpose is highly possible in the near future [8].

3.2. Intervehicle Communication

Refers to the communications that take place among a group of vehicles in a partial or full mesh topology. The requirement for V2V communications comes from the insufficiency of sensors alone in stabilizing the vehicle at high speeds while keeping the intervehicle distance within acceptable ranges. V2V communications impose higher difficulty due to the involvement of more than one vehicle which increases the complexity of communication as well as the vulnerability to security threats. The complexity stems from the nature of data transfer, which can be direct from one vehicle to the other without any intervention of the infrastructure in a single hop but over a short range, or can be relayed over multiple hops (over vehicles or infrastructure) for longer distances. Accident detection, traffic monitoring and Lane Departure Warning System (LDWS) are some of the applications provided by V2V, relying on a variety of technologies like Bluetooth, Wi-Fi, Infrared, and DSRC among others for its implementation.

3.3. Extravehicle Communication

Represents the transfer of information between vehicles and various parts of the infrastructure like edge nodes, RSU and MBS, commonly known as V2I. The information collected by the infrastructure can be useful in traffic monitoring and administration, such as traffic lights detection and fuel consumption optimization. Due to the limited capability of the vehicle's OBU, some services require the intervention of edge servers for task completion. Edge computing plays a vital role in many time-sensitive applications, facilitating a near-vehicle data execution and storage of many real-time services like traffic bottleneck avoidance or pedestrian count for maintaining accessibility and availability without intervention from remote servers.

In addition to V2I, extravehicle communications can also refer to elements in the network other than the infrastructure such as smart Devices (V2D), Pedestrians (V2P), and the Grid (V2G), which are collectively called Vehicle-to-Everything (V2X) communications. Exchanging data with various elements requires a diversity of communication models that are usually wireless, ad-hoc, and bidirectional. Accident prevention and protection for pedestrians and cyclists are some of the most prominent aims of V2X communications, comprising a variety of technologies like mmWave propagation, DSRC, Vehicular Visible Light Communication (VVLC), and Long-Term Evolution (LTE)-V2X cellular standards created by the 3rd Generation Partnership Project (3GPP), which is soon to be evolved to the 5G-V2X cellular systems. Figure 3 demonstrates the various types of vehicular communications.

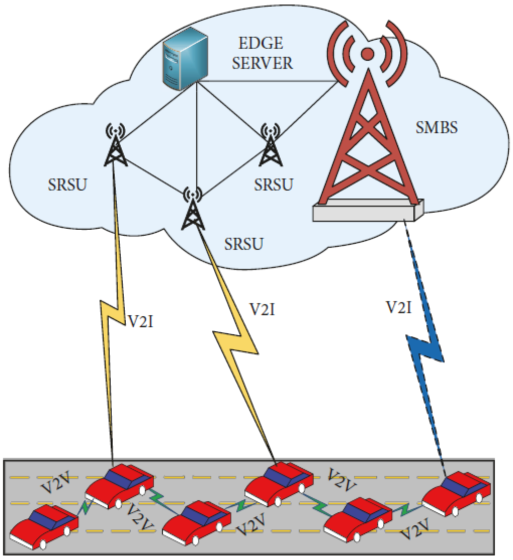

Fig. 3. Depiction of Intervehicle & Extra vehicle Communication

4. ROUTING PROTOCOLS FOR IOAV

Routing plays a vital role in vehicular communications due to the high mobility and heterogeneity in the density of its participating nodes. The requirement for reliable and efficient routing demands a protocol that can govern the numerous numbers of highly mobile AVs as well as other elements in a small geographical area [16]. A routing protocol determines how two networking parties can communicate with each other to exchange their data. They are responsible for route establishment, forwarding decisions, route maintenance, and failure recovery. Latency reduction coupled with the lowest network resource utilization are the major aims of routing protocols in wireless communications [4].

Routing protocols are widely divided, according to the nature of their routing information updating process, into three main categories: Reactive, Proactive, and Hybrid [17, 18, 19] as in figure 4.

4.1. Reactive Protocols

Known as on-demand routing protocols, reactive routing has the routing detection process initiated only upon a message transfer request, eliminating the need to maintain an updated version of the routing information constantly, which reduces the space required to store routing information.

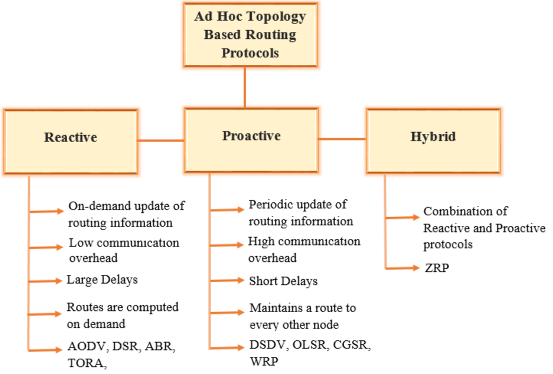
Ad Hoc Topology Based Routing Protocols
Reactive
Proactive
Hybrid
On-demand update of routing information
Low communication overhead
Large Delays
Routes are computed on demand
AODV, DSR, ABR, TORA,
Periodic update of routing information
High communication overhead
Short Delays
Maintains a route to every other node
DSDV, OLSR, CGSR, WRP
Combination of Reactive and Proactive protocols
ZRP

Fig. 4. Ad hoc routing protocols and their characteristics

This non-periodicity in route updating also translates into less bandwidth occupation but at the cost of increasing end-to-end latency, as route establishment must be implemented before exchanging any data packets with other nodes. This is especially intensified when the network is overwhelmed with traffic since the topological information is not shared among the nodes. Ad hoc On-Demand Distance Vector (AODV), Temporally Ordered Routing Algorithm (TORA), and Dynamic Source Routing Protocol (DSR) are well-known examples of reactive routing protocols [17, 18, 20, 21].

4.2. Proactive Routing

Also called table-driven protocols, in which each node preserves one or more routing tables for acquiring a suitable route toward the rest of the nodes in the network. Unlike reactive protocols, the consistency of the routing information is maintained by periodically updating the routing tables and distributing them to the rest of the nodes in the network [17]. Also, in contrast to reactive routing, the constant update in the routing tables would precisely describe the layout of the network without interruptions, minimizing the time required for route formation, which makes them more appropriate for real-time applications. Still, proactive protocols can cause an excessive bandwidth depletion due to the continuous message activity among the nodes, making them unsuitable for environments with dynamic network configurations such as airborne applications, and their applicability decreases as the network's scale and mobility increase to some extent. Currently, some of the most well-known proactive protocols include Optimized Link State Routing (OLSR), Destination Sequenced Distance Vector Routing (DSDV), and Fisheye State Routing (FSR) protocols [17, 18, 21].

4.3. Hybrid Protocols

As previously perceived, Reactive and Proactive protocols have quite opposite pros and cons with each other. In this context, hybrid protocols were developed so that they can enjoy the advantages of both types (i.e. optimizing message exchange rate while maintaining a cap on route formation latency). Hybrid protocols achieve this by partitioning large-scale networks into smaller areas in what is called zone-based routing, where proactive routing is used among nodes of the same zone while the reactive approach is used between nodes of different zones. Zone Routing Protocol (ZBP) is a common example of hybrid routing protocols [20, 21].

In addition to the three aforesaid types, routing protocols can also be classified according to certain node features into five distinct categories: Topology-Based Routing Protocols, which acts based on source and destination nodes, Position-Based Routing Protocols, which uses information based on the geographic area in their routing tables, Cluster-Based Routing Protocols, which distributes the nodes in the network into several separate clusters, Broadcast-Based Routing Protocols, which enable multihop and reliable protocols, and Geocast-Based Routing Protocols, which transfer information to multiple nodes in proximity to each other. The previously mentioned protocols (AODV, TORA, DSDV…) can also be found under this arrangement [16].

5. AUTONOMOUS VEHICLES SERVICES AND APPLICATIONS

The autonomous vehicles networks are developed to provide a wide spectrum of services to their users, which are presented under a variety of applications. Some of these services are built to aid in the undergoing transition from manual to autonomic transportation, like driver assist and road conditions report, others are meant to support fully-automated driving when it becomes the primary means of transportation in the near future. The realization of AV technology on a broader scale can provide plenty of services, some of which are presented as follows [8, 17].

5.1. Safety

The reliability of AV is directly related to the safety of the individuals participating in its framework (passengers, pedestrians, cyclists…). The sensor package fixed on AVs, along with the data supplemented by other vehicles as well as the infrastructure, can cause accident rates to drop significantly, preventing many crash scenarios that may otherwise be unavoidable duo to misjudgement by the human drivers, resulting in a large reduction in traffic delays that may be caused by these accidents.

The exchanged information between the vehicle and its environment can be carried over a variety of messages, such as Basic Safety Message (BSM), and Traffic Message Channel (TMC). The usage of these messages depends on the application of type of AV network being used, like the Fast Healthcare

Interoperability Resources (FHIR) which is typically used for carrying health related information [23, 24].

5.2. Driverless Taxi Services & Car-Sharing Schemes

One of the major services provided by self-driving cars is the autonomous transportation of individuals and goods from one location to another over a large geographical area as part of the overall mobility service featured by smart cities. The elimination of the taxi driver role results in the provision of both the time and money incurred for his services. This can translate to a lot of merits such as reduced transportation cost and better accessibility by multiple individuals, which increases the trend toward taxi sharing or transportation-as-a-service (TaaS) in contrast to individual car ownership. Nevertheless, it also imposes some challenges regarding reduced job opportunities and increased operator responsibilities.

5.3. Increased Road Capacity

Traveling at high speeds while maintaining closer separation among vehicles is one of the prominent properties of AVs. This comes from the conjunction between accurately adjusted breaking and a precise environment observation that allows the vehicles to better utilize the street area without jeopardizing the safety of their occupants. A further step in this direction is when adjacent vehicles line up in platoons to maximize the road’s capacity.

A platoon is comprised of a collection of AVs arranged as a line that rely on a number of technologies for unified means of communication and control, portraying them as if they are a single unit. Platooning has a stabilizing effect on the speed of vehicles, which can result in reduced carbon dioxide emissions as it is directly related to the fuel consumption in traditional vehicles. Platooning can also improve road safety as the essential messages are spread to all members of the platoon in the case of emergencies before initiating the corresponding action by the autonomous system.

5.4. Parking Lots

As the number of vehicles continues to grow, especially in urban areas, so does the need to provide more space dedicated to parking and to distribute it across a large geographical area. Despite being stationary, parked vehicles can still participate in the communication process as infrastructure elements with certain properties, enhancing connectivity by acting as fixed relay points among the vehicles. This is more established by the abundance, wide distribution, and long stationary periods for parked vehicles which enables them to act as if they were static roadside units (sRSU).

Resource sharing is yet another major benefit of utilizing parking lots. When individual vehicles are unable to serve applications with large computational needs due to their limited resources, they can exploit the underused capabilities of parked vehicles to improve the execution time of their given tasks. These can be viewed as temporary processing locations for handling heavier routine tasks.

5.5. Other Services

Since autonomous driving relieves all the occupants from participating in the decision-making process and control over the vehicle, they can exploit their transportation time to perform other valuable activities. It also eliminates the stress resulted from being exposed to the diverse street conditions while driving traditional vehicles and helps to better prepare to the daily life events ahead. Finally, it allows for an additional seat to be occupied that would otherwise be dedicated to the driver.

The ever-accelerated pace of vehicular networks evolution has opened the door to a broader variety of applications that can exploit their platform. As safety represents a priority for AV implementations, applications are classified accordingly into safety and non-safety applications as below [4, 5, 8]:

Safety Applications: Under this branch lies the applications that aim to preserve the safety of the vehicle, its passengers, and their properties and reduce the risk of accidents by monitoring the vehicle's surroundings and taking the necessary measures to avoid any obstacles and smoothly cruise to its destination. Safety applications rely on the sensor pack installed on the vehicle and information received from other vehicles and infrastructure to achieve their purpose.

The information provided regarding the vehicle’s speed, position, and direction is called traveling state information, which can be used by the AV built in technologies like lane switching, blind spot detection, collision avoidance, driver assist or cruise control in both singular and platoon-based traveling modes. Another class of information is triggered as an indication of certain hazardous events, such as changing traffic conditions, emergency braking lights, cooperation or rear-end collisions, and emergency vehicle detection. Relaying this information to nearby vehicles is crucial so they can build a real-time awareness about potential hazards, perform the necessary processing and apply the required actions in due time.

Nonsafety Applications: The infrastructure of AV can also be utilized to provide the passengers with additional applications to improve their AV traveling experience and ease their comfort. These applications usually revolve around two main categories: traffic management and infotainment streaming. The first type is intended to provide more efficient transportation by sharing useful information among vehicles, giving a better traffic flow, road congestion and traffic light operation, avoiding traffic jams, and electing the best route to the designated destination. In contrast, infotainment applications are mainly about providing passengers with location-related data such as the locations of hotels, parks, restaurants and fuel stations. Furthermore, infotainment applications provide internet access to passengers and grant them the ability to partake in a variety of entertainment services, such as video streaming, augmented reality, online gaming, etc...

6. AUTONOMOUS VEHICLE CHALLENGES

The continuous evolution of AV that has been undergoing for the past few years has revealed the presence of many obstacles that may hinder its wide-scale deployment and delay its upcoming realization. These challenges arise due to social and technical motives, originating from the very nature of the AV environment. Although technical challenges are mostly resolved for lower levels of automation, they still persist in higher levels [22]. The main issue to be addressed here is the high mobility and dynamic nature prominent in vehicular networks, which increases the complexity of its activities, coupled with the heterogeneity of the devices connected to it that require a variety of protocols and communication models.

Hardware failures are an issue that negatively affects the wireless components of IoAV. Another degrading factor is the resource limitation problem inherent in many infrastructure components, like battery power, which can be alleviated by utilizing better power management techniques. Routing plays a major role in IoAV communications and can cause serious performance issues if a suitable routing policy that can withstand the dynamic nature of IoAV is not considered [3]. Also, managing the extensive amount of data necessary for AV operation and how to efficiently offload it to edge or cloud servers is a very important topic to be addressed [8].

As with many other wireless implementations, security and privacy are factors not to be overlooked in IoAV communications, since their violation may result in damaging the vehicle or even jeopardizing the lives of its commuters. This is more intensified by the dynamic and flexible nature of IoAV, making it vulnerable to security threats that may not be tangible by a typical IoT framework. These threats can affect privacy, real-time response, and data validation or can inflict various types of jamming attacks to disrupt the flow of information in the network and reduce its reliability [2, 8].

Apart from the aforementioned technical challenges, other class of issues may arise that have its consequences on the social level. These challenges are seen as an unintended outcome resulted from the technical evolution of autonomous vehicles, such as who will hold responsibility in the case of traffic accident, especially if it involves personal injury or damage to property. Also, what basis should be used to discriminate personal from public information, this is particularly important since a huge amount of data is distributed and shared among the vehicles without users' recognition, which is also applicable to incentive-based information. The people's perspective towards AV is another aspect, and whether it is going to be seen as a better or worse replacement to traditional vehicles in people's minds, therefore, a clear and concise image of AV should be drawn that is ought to be comprehensive to all users [3].

7. CONCLUSIONS

In this paper, a brief yet inclusive study has been conducted regarding the communication infrastructure of IoAV. First, a number of IoAV infrastructure models that are suggested by previous studies are presented, emphasizing on the features and tasks of each layer comprising the module. Then, vehicular communications for IoAV are explained, with their associated technologies and examples. The routing protocols used with IoAV are addressed, describing each type with examples and suitable locations of use within the system. Then the services and applications provided by AVs are discussed and classified. Finally, the challenges facing the actual realization of IoAV in the real world are clarified along with any available solutions. The current state of IoAV development does not permit its complete deployment on a broad scale yet, but further collaborative research programs in this direction among academia, government, and industry parties and adopting standardized communication protocols and technologies to ensure interoperability among IoAV networks may hasten the process. The exploitation of various technologies like blockchain, edge computing, artificial intelligence, scalability, reliability, and security and privacy into the IoAV framework may open new insights into its actual utilization for decades to come.

Author contributions: *research concept and design, A.M.H.,A.Q.I.; Collection and/or assembly of data, A.M.H., A.Q.I.; Data analysis and interpretation, A.M.H., A.Q.I.; Writing the article, A.M.H., A.Q.I.; Critical revision of the article, A.M.H.; Final approval of the article, A.Q.I.*

Declaration of competing interest: *The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.*

REFERENCES

1. Tanwar S, Tyagi S, Budhiraja I, Kumar N. Tactile internet for autonomous vehicles: latency and reliability analysis. IEEE Wireless Communications 2019; 26(4): 66-72. https://doi.org/10.1109/MWC.2019.1800553.
2. Nanda A, Puthal D, Rodrigues JJPC, Kozlov SA. Internet of autonomous vehicles communications security: overview, issues, and directions. IEEE Wireless Communications 2019; 26(4): 60-65 https://doi.org/10.1109/MWC.2019.1800503.
3. Jameel F, Chang Z, Huang J Ristaniemi T. Internet of autonomous vehicles: architecture, features, and socio-technological challenges. IEEE Wireless Communications 2019; 26(4): 21-29 https://doi.org/10.1109/MWC.2019.1800522.

4. Peng H, Liang L, Shen H. Li GY. Vehicular communications: a network layer perspective. IEEE Transactions on Vehicular Technology 2019; 68(2): 1064-1078. https://doi.org/10.1109/TVT.2018.2833427.
5. Ahangar MN, Ahmed QZ, Khan FA, Hafeez M. A survey of autonomous vehicles: enabling communication technologies and challenges. Sensors 2021; 3: 706. https://doi.org/10.3390/s21030706.
6. Ali, Qutaiba. Green vehicular ad hoc network (GVANET) project: an efficient deployment of a self powered, reliable and secured vanet infrastructure. IET Wireless Sensor Systems 2018; 8. https://doi.org/10.1049/iet-wss.2018.5112.
7. Shi Y, Lv L, Yu H, Yu L, Zhang Z. A center-rule-based neighborhood search algorithm for roadside units deployment in emergency scenarios. Mathematics 2020; 8(10): 1734. https://doi.org/10.3390/math8101734
8. Raza S, Wang S, Ahmed M, Anwar MR. A survey on vehicular edge computing: architecture, applications, technical issues, and future directions. Wireless Communications and Mobile Computing 2019; 1-19. https://doi.org/10.1155/2019/3159762.
9. Ali QI. Realization of a robust fog-based green VANET infrastructure. IEEE Systems Journal 2022. https://doi.org/10.1109/JSYST.2022.3215845.
10. Islam A, Hossan T, Jang YM. Convolutional neural network scheme-based optical camera communication system for intelligent internet of vehicles. International Journal of Distributed Sensor Networks 2018; 14(4). https://doi.org/10.1177/1550147718770153.
11. Karunathilake T, Förster A. A Survey on Mobile Road Side Units in VANETs. Vehicles 2022; 4(2): 482-500. https://doi.org/10.3390/vehicles4020029.
12. Kaur K, Garg S, Kaddoum G, Kumar N, Gagnon F. SDN-Based internet of autonomous vehicles: an energy-efficient approach for controller placement. IEEE Wireless Communications 2019; 26(6): 72-79 https://doi.org/10.1109/MWC.001.1900112.
13. Wang Z, Guo Y, Gao Y, Fang C, Li M, Sun Y. Fog-based distributed networked control for connected autonomous vehicles. Wireless Communications and Mobile Computing 2020; 1-11. http://dx.doi.org/10.1155/2020/8855655.
14. Boban M, Kousaridas A, Manolakis K, Eichinger J, Xu W. Connected roads of the future: use cases, requirements, and design considerations for vehicle-to-everything communications. IEEE Vehicular Technology Magazine 2018; 13(3): 110-123. https://doi.org/10.1109/MVT.2017.2777259.
15. Eun-Kyu L, Gerla M, Pau G, Lee U, Lim J. Internet of vehicles: from intelligent grid to autonomous cars and vehicular fogs. International Journal of Distributed Sensor Networks 2016; 12(9). https://doi.org/10.1177/1550147716665500.
16. Yogarayan S, Razak SFA, Azman A, Abdullah MFA, Ibrahim SZ, Raman KJ. A review of routing protocols for vehicular ad-hoc networks (VANETs). 2020 8th International Conference on Information and Communication Technology (ICoICT), Yogyakarta, Indonesia 2020; 1-7. https://doi.org/10.1109/ICoICT49345.2020.9166174.
17. Malik FM, Khattak HA, Almogren A, Bouachir O, Din IU, Altameem A. Performance evaluation of data dissemination protocols for connected autonomous vehicles. IEEE Access 2020; 8: 126896-126906. https://doi.org/10.1109/ACCESS.2020.3006040
18. Habelalmateen MI, Ahmed AJ, Abbas AH, Rashid SA. TACRP: Traffic-aware clustering-based routing protocol for vehicular ad-hoc networks. Designs 2020; 6(5): 89. https://doi.org/10.3390/designs6050089.
19. Sasongko AT, Jati G, Hardian B, Jatmiko W. The reliability of routing protocols as an important factor for road safety applications in VANET-based autonomous cars. Journal of Computer Science 2020; 16(6): 768-783. https://doi.org/10.3844/jcssp.2020.768.783.
20. Nazib RA Moh S. Routing protocols for unmanned aerial vehicle-aided vehicular ad hoc networks: a survey. IEEE Access 2020; 8: 77535-77560. https://doi.org/10.1109/ACCESS.2020.2989790
21. Xi C, Tang J, Lao S. Review of unmanned aerial vehicle swarm communication architectures and routing protocols. Applied Sciences 2020;10(10): 3661. https://doi.org/10.3390/app10103661.
22. Shladover SE. Connected and automated vehicle systems: introduction and overview. Journal of Intelligent Transportation Systems 2017; 3: 190-200. https://doi.org/10.1080/15472450.2017.1336053.
23. Wang J, Liu J, Kato N. Networking and communications in autonomous driving: a survey. IEEE Communications Surveys & Tutorials 2019; 21(2): 1243-1274. https://doi.org/10.1109/COMST.2018.2888904.
24. Wolf JC, Jingtao M, Cisco B, Neill J, Moen B, Jarecki C. Deriving signal performance metrics from large-scale connected vehicle system deployment. Transportation research record 2019; 2673(4): 36-46. https://doi.org/10.1177/0361198119838520.

Qutaiba Ibrahim ALI.

Was born in Mosul City, Iraq in 1974. He received the BS and MS degrees from the Department of Electrical Engineering, University of Mosul, Iraq, in 1996 and 1999, respectively. He received his PhD degree (with honor) from the Computer Engineering Department, University of Mosul, Iraq, in 2006. Since 2000, he has been with the Department of Computer Engineering, Mosul University, Mosul, Iraq, where he is currently a full professor. His research interests include computer networks analysis and design, embedded network devices, and network security. He instructed many topics (for post and undergraduate stage) in computer engineering field during the last 20 years and has more than 93 different publications in world class indexed journals and conferences. He acquired many awards and appreciations form different parties for excellent teaching and extra scientific research efforts. Also, he was invited to join many respectable scientific organizations such as IEEE, IENG ASTF, WASET and many others. He was participating as technical committee member in more than 55 IEEE international conferences joined the TPC 10 scientific international journals.
Contact: Qut1974@gmail.com

Mustafa Haitham ALHABIB. Was born in the city of Mosul, Republic of Iraq in 1986, acquired BSc. degree from the Department of Computer Engineering, university of Mosul in 2008, obtained MSc degree in Technical Computer Engineering from the Technical Engineering College, Northern Technical University in 2013. Has over 8 years of academic lecturing in the private sector with 9 research publications in various fields, including Image Processing and Artificial Intelligence. Currently acquiring Ph.D. degree in the field of Intelligent Transportation Systems (ITS) and Connected Autonomous Vehicles (CAV).
Contact: mustafa.20enp4@student.uomosul.edu.iq