Big Data for Autonomous Vehicles

Chapter · April 2021

DOI: 10.1007/978-3-030-65661-4_2

1 author:

Rinki Sharma
M. S. Ramaiah University of Applied Sciences

Big Data for Autonomous Vehicles

Rinki Sharma
rinki.cs.et@msruas.ac.in
Ramaiah University of Applied Sciences

Abstract

Autonomous vehicles (AVs) are going to be integral part of Intelligent Transportation Systems (ITS) in the future. To make AV a reality, it is essential to make the vehicles capable of communication with their surroundings and other vehicles. This gives rise to the Vehicle - to - Everything (V2X) communication scenarios. Realization of V2X communication necessitates real-time intra and inter vehicle communication. Such communication involves high data rate, and leads to enormous data required to be processed in real-time. The big data technologies play a significant role in making AV a reality. This chapter emphasizes the role of big data technologies in AVs. This chapter discusses the enabling technologies and communication protocols for AVs. The components involved in different AV applications and rate at which data is generated for these applications is presented. The role of different big data aspects such as data acquisition, processing, storage, analysis, computing, transmission and security, are discussed by virtue of related research in these domains. With big data for AV being an upcoming research area, the open research issues, important research avenues and ongoing research in these areas is discussed is this chapter with the aim to help the researchers interested in pursuing research in this field.

Keywords

Autonomous Vehicles; Big Data; Vehicular Communication; Intelligent Transportation Systems (ITS); Vehicle - to - Everything (V2X);

List of Abbreviations

5GAA	5G Automotive Association
ABS	Antilock Braking System
ADAS	Advanced Driver Assistance System
AEC	Australian Engineering Conference
AECC	Automotive Edge Computing Consortium
AM	Amplitude Modulation
AV	Autonomous Vehicle
BSM	Basic Safety Message
BT	Bluetooth
CAN	Controller Area Network

CAN-FD	Controller Area Network with Flexible Data Rate
CCN	Content Centric Networking
CD	Compact Disc
C-V2X	Cellular - Vehicle to Everything
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPDA	Dual Polarized Directional Antenna
DSRC	Dedicated Short-Range Communication
ECU	Electronic Control Unit
FM	Frequency Modulation
GPS	Global Positioning System
HVAC	Heat Ventilation and Air Conditioning
ICN	Information Centric Networking
IDS	Intrusion Detection Systems
IEEE	Institute of Electrical and Electronics Engineers
ITS	Intelligent Transportation System
IVN	In-Vehicle Network
JTAG	Joint Test Action Group
LDWS	Lane Departure Warning System
LIDAR	Light Detection and Ranging
LIN	Local Interconnect Network
M2M	Machine to Machine
MANET	Mobile Ad-hoc Network
MITM	Man In The Middle
ML	Machine Learning
MOST	Media Oriented System Transport
MU-MIMO-OFDM	Multi User - Multi Input Multi Output Orthogonal Frequency Division Multiplexing
NDN	Named Data Networking
NDVN	Named Data Vehicular Network
NFV	Network Function Virtualization
NHTSA	National Highway Traffic Safety Administration
OBD	On Board Diagnostics
OTA	Over the Air
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RDS	Radio Data System
RSU	Road Side Unit
SAE	Society of Automotive Engineers
SDN	Software Defined Networking
SDVN	Software Defined Vehicular Network
TCP	Transmission Control Protocol
TCU	Transmission Control Unit
UDP	User Datagram Protocol

USB	Universal Serial Bus
V2C	Vehicle to Cloud
V2D	Vehicle to Device
V2G	Vehicle to Grid
V2I	Vehicle to Infrastructure
V2P	Vehicle to Pedestrian
V2R	Vehicle to Roadside
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VANET	Vehicular Ad-hoc Network
VLC	Visible Light Communication
V-NDN	Vehicular - Named Data Network
WAVE	Wireless Access for Vehicular Environments
WSMP	WAVE Short Message Protocol

1.1 Introduction:

Over the years there has been tremendous advancement in vehicular technology. Network and communication technology made its way into the vehicles for applications such as comfort, driver assist and fleet management. Gradually vehicle communication is advancing towards vehicle - to - everything (V2X) scenario. Under V2X communication, a vehicle is capable of Vehicle - to - Vehicle (V2V), Vehicle - to - Infrastructure (V2I), Vehicle - to - Cloud (V2C), Vehicle - to - Pedestrian (V2P), Vehicle - to - Device (V2D) and Vehicle - to - Grid (V2G), to name a few. There are standards and protocols defined to enable such communication. Enabling vehicles to communicate with their surroundings eventually aims to achieve an autonomous vehicle (AV), capable of maneuvering itself depending on its surroundings [1]. Realizing an AV requires high rate Intra and Inter vehicle communication over different interfaces of the vehicle. This leads to generation of enormous data, that needs to be processed at a very high rate. This is where big data technology plays a significant role in AVs.

This chapter aims to emphasize upon the importance of big data technologies in AVs. AVs are going to be a reality in future, and it will lead to generation of enormous data. Technologies should be made capable of communicating, storing and processing such data efficiently, reliably and securely. This chapter presents the enabling communication technologies and protocols for AVs. There are different protocols and technologies for different applications. The protocols and standards for vehicular communication, along with their supporting data rates are discussed in detail. Based on the levels of automation of an AV, the complexity and generated data increases. The components involved for different AV applications and rate of data generation is presented. After getting the clarity on big data generation of AV, the aspects of big data such as big data acquisition, processing, storage, analysis, computing, transmission and security, are discussed by virtue of related research in these domains. As big data for AV is an upcoming research area, there are many open research issues in this field. Lastly, some of the important research avenues in this field are presented.

1.2 Vehicular Communication:

Vehicular communication is an integral part of the future Intelligent Transportation Systems (ITS). ITS comprises of intelligent vehicles capable of communicating with their surroundings and other vehicles that are within communication range. Eventually this trend will lead to self-driving or autonomous vehicles [2]. Intelligent vehicle applications can be broadly classified into the following four major areas:

1. **Convenience:** Aimed to assist the driver with safe and comfortable driving, applications such as infotainment, night vision assist, seat and mirror control, 360° camera, nearby services (restaurants, gas station, emergency etc.) and navigation assist fall in this category.

2. **Safety:** Advanced Driver Assistance Systems (ADAS), blind spot assist, lane detection and cruise control, vehicle platooning, crash detection, pre-safe brake are some of the applications that fall in this category.

3. **Productivity:** This applies to commercial and transit vehicles. Applications such as fleet management wherein parameters such as location, speed, mileage, drive time, idle time, stop time, trip reports of fleet and transit vehicle is traced and tracked to ensure efficient and productive maneuvering.

4. **Traffic assist:** This is used for improved and smooth traffic flow in case of crash and congestion. Road crashes are ‘spot disasters’, while traffic congestion is a ‘distributed disaster’, both affecting the smooth flow of the traffic. V2V and V2I communication is significant in propagating the information about crashes and traffic congestion. Based on this information, alternate routes can be used and the traffic can be diverted to appropriate routes, thus achieving smooth flow of traffic.

Vehicular communication implies of communication considering vehicles or the Electronic Control Units (ECUs) within the vehicle as the communication entities. Broad classification of vehicular communication is presented in Figure 1.

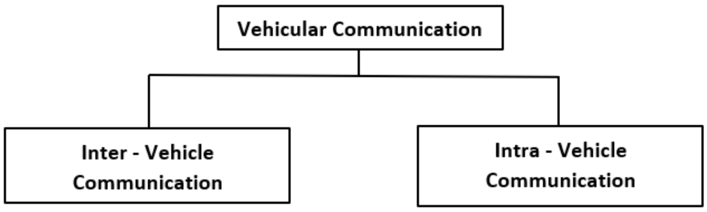

Figure 1: Classification of Vehicular Communication

Vehicular communication can be broadly classified as:

1. **Inter - vehicle communication**
    a. Primarily used for ITS applications such as convenience, safety, productivity and traffic assist. Inter - vehicle communication comprises of communication between vehicles as well as between vehicles and infrastructure. Some examples of Inter - vehicle communication are V2V, V2I, V2C, V2P, V2D and V2G, together represented as V2X communication [3]. By using inter-vehicle communication techniques, vehicles can communicate with each other for platooning / collision avoidance. A vehicle can communicate with roadside infrastructure, pedestrian or cloud for dynamic traffic signaling, transmission of safety alerts, real-time traffic and weather updates, road condition-based navigation and other cloud services. When two or more vehicles come within communication range of each other, they form an adhoc network and exchange data. Such networks are called as vehicular adhoc networks (VANETs). VANETs are a subset of mobile adhoc networks (MANETs), wherein the mobile nodes are vehicles having a pre-determined and uniform mobility pattern (unlike random mobility of MANETs) [4].

2. **Intra - vehicle communication**
    a. Intra-vehicle communication is also known as in-vehicle communication. It takes place within the vehicle, between its ECUs, sensors and actuators. Depending upon the application and required data rate, different in-vehicle networking protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented System Transport (MOST), FlexRay and Automotive Ethernet are used for communication between the components within the vehicle [5]. Details of in-vehicle networking protocols, their applications and required data rates are presented in Table 1.

1.3 Protocols and Standards for Vehicular Communication:

With the aim to make high speed exchange of data possible for inter - and intra - vehicle communication scenarios, numerous standardization activities have taken place. Among the frontrunners to develop protocols and standards for vehicular communication are Institute of Electrical and Electronics Engineers (IEEE) [6], Society of Automotive Engineers (SAE) [7] and 5GAA (5G Automotive Association) [8]. Apart from the standards developed by these groups, technologies such as Bluetooth and Visible Light Communication (VLC) are also used for short range vehicular communication [9]. The in-vehicle network communication protocols enable communication among the components within the vehicle. This section presents the protocols and standards used for vehicular communication.

1.3.1. Dedicated Short-Range Communication (DSRC)

IEEE and SAE worked together to develop the Dedicated Short-Range Communication (DSRC) standard for vehicle - to - vehicle (V2V) and vehicle - to - roadside (V2R) also known as V2I communication. DSRC standard comprises of Wireless Access for Vehicular Environments (WAVE), IEEE 802.11p amendment for vehicular environments, the 1609.2, 1609.3, 1609.4 standards for resource management, security services, networking services and multi-channel operations respectively [10]. While the communication stack is developed by IEEE (being the pioneers in network communication), the messages to be exchanged based on the application are defined by SAE. The SAE J2735 standard presents the message set dictionary and SAE J2945.1 standard defines the minimum communication performance requirements [11]. The layered architecture for DSRC standard is presented in Figure 2.

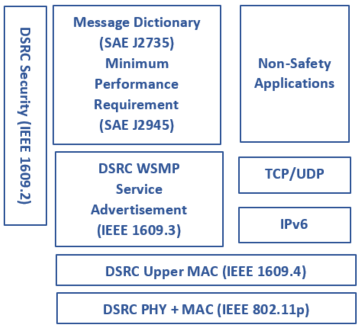

Figure 2: Layered Architecture of DSRC

DSRC operates at the 5.9 GHz frequency band that spans from 5.850 GHz to 5.925 GHz. The short to medium range communication can go up to 1000m (1km). The supported V2V and V2R communication environments can be used for applications such as broadcasting localized traffic or road information directly into the vehicle, highway advisory radio, emergency vehicle approach warning and impending collision warning, to name a few. The choice between using WAVE Short Message Protocol (WSMP) or IPv6+UDP/TCP depends on the requirements of a given application [12].

The protocols in the DSRC layered architecture and their functionalities are as follows:

- **IEEE 802.11p: Medium Access Control and Physical Layer Specifications for WAVE**
  - Amendment to 802.11 to enable operation without setting up a basic service set
  - Physical layer for implementing DSRC [13]

- **IEEE 1609.4: Multi-Channel Operations**
  - Coordinate switching between the control channel and service channels
  - User priority access to the media
  - Routing data packets on the correct channel [14]

- **IEEE 1609.3: Network Services**
  - Defines network and transport layer services, including addressing and routing
  - Examples of message types are WAVE short Messages, WAVE service advertisements, and WAVE routing advertisements [15]

- **IEEE 1609.2: Security Services for Applications and Management Messages**
  - Defines secure message formats and processing
  - Messages to be protected from attacks such as eavesdropping, spoofing, alteration, and replay [16]

- **SAE J2735: DSRC Message Set Dictionary**
  - Specifies message sets, data frames, and data elements
  - Support interoperability among DSRC applications
  - Defines Basic Safety Message (BSM) [17]

- **SAE J2945/1: On-Board System Requirements for V2V Safety Communications**
  - Specifies the system requirements for an on-board Vehicle-to-Vehicle (V2V) safety communications

– Addresses BSM transmission rate and power, accuracy of BSM data elements, and channel congestion control [18]

As the physical layer standard WAVE is based on the 802.11 family of standards, the supported data rates depend on the 802.11 standards. The latest 802.11 standard is 802.11ax, also known as Wi-Fi 6 that uses Multi User - Multi Input Multi Output - Orthogonal Frequency Division Multiple Access (MU-MIMO-OFDMA). It can support data rates of up to 600 Mbps (80MHz bandwidth, 1 spatial stream) and 9607.8 Mbps (160 MHz bandwidth, 8 spatial streams) [19].

Table 1: In-vehicle Network Protocols

Protocol	**Supported Data Rate**	**Applications**
Controller Area Network (CAN)	1 Mbps	Engine management, cruise control, transmission control, ABS, HVAC
CAN with Flexible Data Rate (CAN-FD)	15 Mbps	Airbags, antilock braking system (ABS), X-by - wire, all applications handled by CAN
Local Interconnect Network (LIN)	20 kbps	Control of door, window, seat, mirror, sunroof. Diagnostics.
Media Oriented System Transport (MOST)	25 Mbps	Infotainment, navigation
FlexRay	10 Mbps	X-by-wire, airbags, antilock braking system (ABS)
Automotive Ethernet	10 Mbps to 1 Gbps	Backbone network, 360° camera, systems for infotainment, powertrain, ADAS, body comfort, chassis safety and diagnostics

1.3.2 Cellular V2X

Cellular V2X (C-V2X) standard is developed by 5GAA that works towards roadmap for 5G connectivity for vehicular communication. This standard has evolved from 3GPP standardized 4G LTE (Long Term Evolution) and 5G mobile cellular connectivity. C-V2X is considered to be capable of supporting highly reliable real-time communication at high speeds, in high-density traffic. Since this standard has evolved from 3GPP standards with established infrastructure all over the world, it reduces the cost of infrastructure deployment and benefits from cellular network densification. 3GPP support of ITS 5.9 GHz band. C-V2X and 802.11p can co-exist by being placed on different channels in the ITS band. The data rate and communication range are comparable with DSRC [20].

1.3.3 Bluetooth

The IEEE 802.15.1 standard, works in the unlicensed band of 2.4 GHz and supports 1 Mbps data rate for voice and data. It supports short range vehicular communication for up to 10m distance. In vehicles, Bluetooth is used for wireless sensors and cable replacement [21]. Seat occupancy detection, mirror control, smart vehicle access (key fob control), personalization and infotainment control, assisted car parking and work zone indication through Bluetooth enabled barricades are some of the applications supported by Bluetooth in vehicular environments.

1.3.4 Visible Light Communication (VLC)

Supported by the IEEE 802.15.7 working group, VLC supports short range Line of Sight (LoS) communication. Visible light communication (VLC) uses visible light between 400 and 800 THz (780–375 nm). Fluorescent lamps can transmit signals at 10 kbps. LEDs can support data rate of up to 500 Mbps over short distances [22]. V2I communication is possible between traffic light and vehicle head lights while V2V communication is enabled through head light of a vehicle to tail lights of the preceding vehicle. Outdoor advertising on mobile nodes is another application of VLC.

1.3.5 In-vehicle communication protocols

A modern luxury car can have as many as 150 ECUs [23], that can handle complex and significant applications such as cruise control, engine management system, airbags, antilock braking system (ABS), heating ventilation and air conditioning (HVAC) that require high reliability and data rate, to simple tasks such as mirror control and seat adjustment. Infotainment systems in the car provide real-time data transmission that requires high data rates. Different protocols are used based on varying requirements of the applications. Table 1 presents the most popular wired protocols used for in-vehicle communication, their applications and data rates. As discussed in Section 1.3.3, Bluetooth wireless communication protocol is also used for in-vehicle communication.

1.4 Autonomous Vehicles (AVs)

An autonomous vehicle (AV) can be defined as the one that can drive itself from one point to another predetermined destination in ‘autopilot’ mode, using various in-vehicle and inter-vehicle communication technologies and applications, GPS navigation, sensors, lasers and radar. Use of AV is expected to rise considerably in coming years as they are expected to increase road safety and travel time efficiency.

Some of the advantages of using AVs are as follows:

1. **Road safety:** According to the study by National Highway Traffic Safety Administration (NHTSA), 94% of road accidents are caused by human error. Some of the main causes of human error while driving are over speeding, reckless driving, inattentiveness, intoxication, impaired and underage driving.

2. **Travel time efficiency:** Travel can be more productive for people when most of the driving decisions are automated. AVs use navigation and communicate with surrounding vehicles and infrastructure, which makes them capable of identifying road conditions, accidents or delays thus choosing better routes to destination.

3. **Reduced air and noise pollution:** Vehicular pollution is one of the main causes of increase in carbon monoxide and nitrogen oxide in the air. Slow moving traffic and congestion leads to high fuel burning leading to air pollution. Excessive honking or congested roads cause noise pollution. AVs would reduce this drastically through intelligent navigation and communication with surrounding vehicles and infrastructure.

1.4.1 Levels of Automation:

SAE J3016 defines six levels of automation. The details of these levels are as follows [24]:

1. **Level 0 (L0):** These are the basic cars without any form of automation.

2. **Level 1 (L1):** Supports low level driver assistance systems. Vehicles with features such as lane departure assist and adaptive cruise control fall under this category. BMW’s driver assistance systems are an example of L1 automation.

3. **Level 2 (L2):** This level provides partial driving automation. Advanced Driver Assistance Systems (ADAS), wherein a vehicle can control both

steering and acceleration / deceleration of the vehicle, fall under this category. Tesla's Autopilot and General Motor's Cadillac are examples of vehicles having L2 of automation.

4. **Level 3 (L3):** This level supports conditional driving automation. L3 vehicles are capable of 'environmental detection' and make informed decisions. However, the driver is required to be alert and is allowed to take control of the system if necessary. Audi's A8 is a L3 vehicle.

5. **Level 4 (L4):** These are high driving automation vehicles wherein the vehicle itself is capable to intervene in case of system failure, requiring no or minimal human interaction. While, L4 vehicles can operate in self-driving mode, there is still an option of manual control. Most of the L4 vehicles are being developed for taxi and ridesharing purposes. Some of the examples of L4 vehicles are shuttles and cabs by French company NAVYA, self-driving taxi by Waymo and Magna, and robotaxi by Volvo and Baidu.

6. **Level 5 (L5):** These vehicles support full-driving automation and require no human control. These vehicles won't even have steering wheels or brakes, and will be free from geofencing. These vehicles are under test.

1.4.2 Big Data Sources for Autonomous vehicle

AVs are capable of making informed decisions and self-drive because they constantly communicate with vehicles and infrastructure within their communication range, Global Positioning System (GPS), as well as the cloud [25].

The primary big data generation sources, related components and their applications are presented in the Table 2.

Table 2: Big Data Generation Sources

Technology/ Domain	Components	Applications
Imaging for Automotive	Visible cameras 3D cameras Night vision cameras LIDAR Long-range radar Short-range radar Dead reckoning sensors Ultrasound GPS	Blind-spot Side-view (mirrorless cars) Stereo cameras: direction and distance for Lane Departure Warning System (LDWS) Traffic sign recognition Gesture recognition Presence detection Driver monitoring Pedestrian / animal detection 3D mapping of surroundings

		Adaptive cruise control Front and rear parking Odometry Parking Pedestrian and obstacle detection (Short Range) Positioning and navigation
Cloud	Data servers Roadside infrastructure	High Definition Maps Infotainment Vehicle sensor data Crowdsensing data Edge caching data Over the Air (OTA) updates Road condition updates
Vehicular Adhoc Network Communication (VANET)	Wireless communication module	Cooperative driving Platooning Road condition updates (wet road, collision, braking, road maintenance) E-toll Location based advertising Retail promotion
In-vehicle network data	Electronic Control Unit (ECU) Sensors Actuators In-vehicle network	Engine control Tire pressure monitoring Transmission control Anti-lock braking Body control HVAC Infotainment X-by-wire Airbag Diagnostics ADAS Adaptive cruise control Seat and mirror control Backbone networks Gateways

According to a study at Australian Engineering Conference (AEC), 2018, an autonomous vehicle will generate around **166 Giga Bytes of data per hour,** and around **4000 Giga Bytes of data per day** [26]. Real-time applications such as traffic management, navigation, autonomous driving, toll collection, vehicular communication, review of vehicle performance and predictive maintenance, location-based promotion and advertising to name a few, require high data rate and bandwidth for acceptable operation and performance.

1.5 Big Data in AV

As seen from the examples of data generation in AVs, thousands of Giga Bytes of data per day will be produced and communicated in a network of AVs. Advanced, efficient and robust techniques and technologies are required to handle such big data in terms of its acquisition, transmission, storage, computation, analytics and processing. This section discusses these aspects of big data processing.

1.5.1 Big data acquisition:

As discussed in the previous sections, AV related data needs to be acquired through diverse sources, such as sensors, cameras, wireless communication technologies and in-vehicle network, in various V2X scenarios. It is important to ensure that the acquired data does not compromise information about driver or passengers. Therefore, ensuring security and privacy of the acquired data is crucial. The heterogeneity of data source presents several challenges in the data acquisition process, such as security and privacy issues, coverage area, cost to obtain data and corporate/government policies. Data scalability is a matter of concern in vehicular networks as the participants have limited resources. The computational infrastructure of the vehicle needs to be capable of storing and processing huge amounts of heterogeneous data [27,28].

1.5.2 Big data preprocessing:

AV data is acquired through heterogeneous sources at a high rate of data generation as seen in previous sections [28, 29]. Vehicular data obtained from different sources is in raw form, and needs to be processed before it can be brought to use. Data preprocessing can be carried out in five steps [30, 31, 32]:

1. **Data cleaning**
    a. Filling missing values
    b. Smoothening noisy data
    c. Confirmation and removal of outliers

2. **Data integration**
    a. Integrating data and converting into consistent data type

3. **Data transformation**
    a. Normalization, aggregation and summarization of data

4. **Data reduction**

    a. Reducing the size of the data

5. **Data discretization**
    a. Converting numerical values into categorical values

1.5.3 Big data storage:

Traditional data storage systems such as Redundant Array of Independent Disks (RAID) are not suitable for vehicular networks and AVs because they are less reliable, less secure, and not designed to scale up to enormous data generated by these applications [33]. The data storage for AV and vehicular networks is required to have the following characteristics:

1. **Availability:** All time availability of data regardless of downtime

2. **Scalability:** Capable of storing the ever increasing amounts of data

3. **Security:** Data confidentiality and authenticated access over multiple drives, servers, containers and locations

4. **Efficiency:** Should be capable of managing Petabyte - Exabyte of storage

5. **Cost effectiveness:** Reduced cost of ownership and replication

The following three types of storage is used for vehicular big data [34, 35, 36]:

1. **On-board storage:** Used to store data locally. Because of local storage, data can be accessed in real-time.

2. **Roadside storage:** Roadside infrastructure is preoccupied with storage. Data can be buffered and relayed for longer distances to the receiver that are not in direct communication range of the vehicle. Vehicle can also download data through roadside infrastructure. However, it adds to transmission delays. Location based advertisement of the nearby services use roadside infrastructure.

3. **Internet storage:** Vehicles communicating through internet to exchange important information such as weather, Over The Air (OTA) updates and infotainment, are some of the example use cases for this type of storage.

Based on access mechanisms, vehicular data storage can be classified into the following:

1. **Fast access:** Used for delay sensitive applications where data is accessed within a guaranteed delay. For example, data for vehicle safety and autonomous driving.

2. **Medium access:** Comprises of external storage that can be accessed through a reliable connection. For example, storage access through multi-hop communication and backhaul transmission. V2V assisted content delivery schemes, where the storage memory of a forwarding vehicle caches the popular content temporally until it comes across another forwarder is an example of medium access vehicular data storage.

3. **Slow access:** This is the external storage that can be accessed through an opportunistic connection due to mobility of vehicle and unavailability of consistent connection causing delays. Roadside infrastructure can be used for data storage for vehicles. Cloud storage is used to store data beyond local storage capacity and to improve utilization of overall vehicular resources. For example, V2R and V2C communication.

1.5.4 Big data analysis:

As the idea of connected and autonomous vehicles may soon become a reality, researchers believe that the data analysis and storage requirements of AV pose challenge to the capabilities of most of the big data solutions available at present [37]. Analysis of the data produced and communicated for an AV needs to be analyzed and processed in real-time to safely navigate the vehicle. This helps in revealing hidden patterns, unknown correlations, driver behavior and preferences to make informed decisions in real-time [38]. The vehicle needs to choose from different data streams in real-time and analyze the most appropriate data stream based on the requirement. Therefore, an AV needs to run machine learning and analytics engines to recognize critical data and analyze it in real-time.

Hence, the data analytics and machine learning algorithms for AV should be able to:

1. Recognize critical data for a given scenario

2. Perform real-time data analysis

3. Compress and aggregate non-critical data for caching and future use

4. Periodically upload non-critical data to cloud for future analytics

5. Support download of required data from the cloud, process in real-time and act appropriately

In levels 1 - 4 of autonomy supported in an AV, data analytics can guide the driver through driving decisions and safely navigate the vehicle depending on driver's behavior.

Such data analytics can be classified into three types:

1. **Descriptive analytics:** With the help of techniques such as data aggregation and data mining, descriptive analytics summarizes the historical data, which is used to identify behavioral patterns and relationships. This information provides vital understanding of information about the behavior of different parameters across a variety of fields and industries.
   In case of AV, descriptive analytics applies to moment-to-moment driving patterns and road behavior of the driver. This is aimed to study safe and risky behaviors of the driver.

2. **Predictive analytics:** While descriptive analytics identifies behavioral patterns based on historical data, predictive analytics is a method to identify the prospect of future outcomes. Predictive analytics assesses the future events by using data analytics and machine learning techniques on the historical data.

   In case of AVs, based on the past driving patterns and road behavior, the vehicle can make informed judgement of driver's possible behavior in a given situation. For example, given the proximity with other vehicles or obstacles, whether the driver will slow down, overtake, navigate through or brake.

3. **Prescriptive analytics:** Based on the information obtained through the descriptive and predictive analytics, prescriptive analytics works towards establishing the actions to be taken in the future for a given scenario.

   For the AV environment, prescriptive analytics uses the information obtained through descriptive and predictive analytics and issues recommendations based on driver's behavior in the past. The vehicle can assess the risk for a given situation and suggest appropriate action in real-time.

1.5.5 Big data computing:

In an AV, most of the operational decisions need to be made by the vehicle instead of the driver (depending on the level of automation). In such a scenario, real-time decision making with reliability and security is paramount. To make real-time decisions, the level of functionality of automotive computing systems and computer processing needs to be increased [35, 37].

To enable AV functionality, the vehicles need to have the following characteristics:

1. **High computing power:** Approximately 1GB of data will need to be processed and analyzed every second, and real-time decisions will need to be made within a fraction of second. This demands for high computing power at the vehicle.

2. **Centralized computing:** In most of the present day vehicles, different ECUs of the vehicle carry out their own computation, leading to a distributed computation architecture. As the decision making dependability among different ECUs increases, a centralized computing approach will be more efficient by reducing processing complexity, thus achieving real-time decisions.

3. **Small, high-processing units:** Multiple computing components will need to be installed at different places in the vehicles. Hence, these computing units will need to be small in size while providing high processing power.

4. **Security and privacy:** As applications communicate with roadside infrastructure, other vehicles and over cloud, it is essential to ensure that communicated data is secure and there are no malicious nodes in the communication link.

Edge computing for vehicular networks:

As discussed earlier, AVs generate and process huge volumes of data. Present mobile communication network architectures and cloud computing systems are not capable of handling such huge volumes of data. Network architecture based on topology aware computing and storage resources could be a solution for highly dynamic vehicular networks [38]. For such scenarios, topology-aware distributed clouds with multi operator edge computing capabilities is a solution suggested by the Automotive Edge Computing Consortium (AECC) [39]. Edge is the hierarchical distribution of non-central clouds and their computational resources in a flexible and topology aware manner. Real time applications require faster computing. In case a vehicle is not equipped with sufficient resources, it can use the resources available with the nearest regional edge infrastructure, instead of sending the computation request all the way to a central cloud. This edge infrastructure is distributed over the network at different locations / regions to cater to the needs of mobile nodes. Some architectures propose the use of computing resources of other vehicles (V2V) or of roadside infrastructure (V2R / V2I). Common services that can use edge computing for real-time data computing are intelligent / assisted driving, in-vehicle infotainment and OTA.

1.5.6 Big Data Transmission

As seen in previous sections, thousands of Giga Bytes of data is generated and exchanged per day by a single AV. In a network of such vehicles this data increases multiple times. Most of the vehicular data is real-time and needs technologies that support high bandwidth and data rate. Communication and networking technologies have to be capable and efficient enough to handle such huge data reliably and without delays (for real-time applications in particular). IEEE and 5GAA are the standardization bodies working in this direction. The protocols and standards used for vehicular communication, and their supported data rates are presented in Section 1.3. Density of vehicles in urban areas is high while their mobility is usually low (due to traffic congestion). While in rural areas, vehicle density is less and mobility is high. The study carried out in [40] presents the variation in bandwidth requirement of such different scenarios. As the number of AVs on roads increase in future, the demand for high bandwidth, data rates and efficient technologies will keep on increasing. Continuous efforts are being made by the research community to enhance efficiency and data rate of communication technologies.

Authors in [41] present the terahertz communication model for increase in network bandwidth. This model operates in 0.1 - 1 THz frequency band. Since this band is not used by many communication technologies, data transmission in this channel is relieved of interference. However, limitation of this channel is short range and line-of-sight communication, that makes this band unsuitable for vehicular communication. Vehicular networks use multi-hop communication. Hence, efficient cross-layer solutions (physical, Medium Access Control (MAC), and network layer solutions) are needed. Directional antenna / beamforming is used by the IEEE 802.11n, 802.11ac, 802.11ad (WiGig) to increase communication range and reduce interreference. However, using beamforming leads to the problem of deafness [42]. A cross-layer solution presenting the benefits of use of dual polarization with beamforming are presented in [43]. This solution simultaneously uses two orthogonal polarizations (vertical and horizontal polarizations) for data transmission. Since the data is transmitted over orthogonal polarizations, the signals do not interfere (as long as the orthogonality is maintained) while achieving data rates higher than cases where only single polarization is used. The Dual Polarized Directional Antenna (DPDA) based MAC layer solution is presented in [44]. The DPDA based multi-hop, multipath routing protocol is presented in [45].

Whether the application is connectionless (User Datagram Protocol (UDP) based) or connection oriented (Transmission Control Protocol (TCP) based), the traffic load on the network, affects the performance of the network [46]. Certain applications require higher data rates compared to others. For example, infotainment and navigation require higher data rates compared to location based commercial updates. Therefore, it is required to develop application-based transmission strategies. [47].

1.6 AV security:

An AV makes driving decisions based on its surroundings. It also communicates with other vehicles and roadside units in its vicinity. These vehicles have applications that require them to exchange information over edge / cloud computing platforms as well, as discussed in earlier sections. As more and more electronics, intelligence features and communication interfaces are integrated in the vehicle, the more vulnerable the vehicle becomes to malicious actions [48, 49, 50].

With increase in the number of ECUs in the vehicle, and availability of interfaces to access the ECU through wireless communication, in-vehicle network with access interfaces such as Universal Serial Bus (USB) and diagnostics port, it becomes easy to hack the vehicular components and networks. This also compromises the driver / passenger information of the vehicle [51].

The vehicle interfaces susceptible to exploits are as follows:

1. **Direct access interfaces:** Infotainment systems, Compact Disc (CD) player, on-board diagnostics

2. **Short-range wireless communication interfaces:** Remote keyless entry, tire pressure monitoring, Bluetooth, Wi-fi

3. **Long-range wireless communication interfaces:** Satellite radio, AM/FM radio, cellular communication, edge / cloud platform access

Table 3: Threats on Vehicular Networks

Threats to Vehicle	Method	Possible Interfaces to access the network
Man In The Middle (MITM) Attack	Intercept, modify and resend the information	CAN/BT/WiFi/ Cellular/OBD
Denial of Service (DoS) Attack	Delete encrypted premium content, Flood the network	Unauthorized applications from remote device or downloaded to the infotainment system

Replay attack	Replay V2X messages, Replay in-vehicle messages	V2X/ IVN/ OBD
Collect private information	Record vehicle messages, Track vehicle's location and transactions, Infer private information about driver and passengers	V2X/GPS
Unauthorized control of vehicle parameters	Install program onto vehicle's IVN bus	OBD/ USB
False alerts	Transmission of false hazard warnings Injecting RDS-TMC (Radio Data System- Traffic Message Channel) traffic information signals	RDS / TMC / V2V
Conceal location information	Use GPS jamming device preventing fleet owner from tracking the fleet	GPS
Tamper ECU data	Change ECU configuration, Modify calibration file, Tamper persistent database	OBD / CAN / JTAG
Bluejacking and Bluebugging	Send unsolicited messages over Bluetooth	BT

A hacker can find a vulnerable ECU (which could be accessed remotely), reprogram it thus compromising the ECU, and send malicious content to other ECUs in the network through vehicle bus or other interfaces. This way the hacker can obtain control on the vehicle. Table 3 shows the list of threats on vehicular networks.

Some of the techniques that can be used to mitigate these attacks over V2X and IVN systems are:

1. Message encryption and authentication

2. Firewall to restrict communication between networks

3. Securing the gateway modules that are used to facilitate communication between different IVN protocol networks

4. Intrusion detection and prevention systems to detect and prevent malicious content

5. Securing the safety critical systems such as braking, engine control unit and steering control unit

6. Securing the infotainment systems such as telematics, in-vehicle infotainment (IVI) and radio system
7. Secure firmware update
8. Secure hardware

1.7 Research avenues

Vehicular networks and AVs are the upcoming technologies and have caught interest of numerous researchers all over the world. The research on big data in AV primarily deals with transmission of big data, studying the available data, storage and computation, and data security. This section presents some of the research avenues and related research works in this field.

1.7.1 Big data transmission

The communication technologies for AV need to support high data rate and bandwidth to allow real-time communication in different V2X scenarios. Research community is constantly working towards developing solutions based on standard vehicular communication standards. Physical, MAC and network layer routing solutions are needed for efficient bandwidth usage and interference avoidance, channel access and routing of information over a network respectively. Many of the existing solutions have been discussed in Sections 1.3 and 1.5. Some of the latest research avenues are discussed here:

Information Centric Networking (ICN): Traditional networking communication is address based, wherein the source (client) sends request to the destination (server) and receives a reply. In highly dynamic vehicular networks, information is given importance, instead of where it is coming from. Information such as real-time vehicle status, road conditions, weather information (usually available in the cloud), is required with minimal delay. ICN allows intermediate nodes or roadside infrastructure to store this information. On receiving the query for such information, a node or roadside infrastructure having latest information for the query replies with information, instead of sending the query all the way to server/cloud [52, 53]. This drastically reduces delay and helps in efficient use of bandwidth. Content Centric Networking (CCN) is also referred to as Named Data Networking (NDN) and is one form of ICN that supports name-based data retrieval and pervasive caching. The concept of NDN applied to vehicular networks has given rise to Vehicular - NDN (V-NDN) or Named Data Vehicular Networks (NDVN) [54, 55]. In this field, content naming, caching and forwarding schemes need to be developed.

Some of the open research issues in this domain are:

1. **Development of routing strategies:** Efficient routing mechanisms needed to fulfil QoS requirements of vehicular network.

2. **Content naming schemes:** Appropriate content naming schemes need to be developed for vehicular networks.

3. **Caching strategies:** Intermediate nodes and roadside units can cache the data, but there are no standard schemes about storing and forwarding of data.

4. **Interest and data flooding:** Method and periodicity for flooding of interest and data packets needs to be standardized.

5. **Approach to handle dynamic network topologies:** Topologies in vehicular networks change constantly leading to disruption of connection. Solutions to overcome this problem are required.

6. **Security in V-NDN/NDVN:** Authentication and encryption add substantial overhead. There is a need to develop light weight solutions for secure communication [56].

Software Defined Networking (SDN) and Network Function Virtualization (NFV):

Big data generated by AVs and vehicular networks will need high bandwidth, storage and computing power. The individual vehicle may lack enough storage and computing power for all the generated data. In such cases, edge and cloud computing, and virtualization of network resources will play a crucial role in reducing CAPEX and OPEX of vehicular networks [57, 58, 59]. Traditional network technology is not efficient enough to handle the volumes of data generated by AVs. SDN allows dynamic configuration of network resources based on the need and achieves better QoS in a vehicular network scenario when compared to the traditional networking architecture. Many researchers have proposed Software Defined Vehicular Network (SDVN) architectures [60]. Some of the benefits of SDVNs are dynamic network configuration, better resource utilization, reduced latency and integration of heterogeneous networks through network controller.

While SDVNs provide these benefits, the highly dynamic nature of vehicular networks along with huge data produced and communicated over wireless medium leads to the following challenges, with need to develop solutions:

1. **Mobility management:** This leads to varying channel conditions. SDN paradigm needs to be modified to handle the issues of network mobility and connection breakages. To ensure constant network connectivity and maintain required QoS, the SDN based solutions need to predict the driving patterns and pre-allocate resources while handling the concerns of privacy.

2. **Lack of standardized APIs to handle heterogeneous network traffic:** SDN network controller provides separation between applications and network infrastructure. However, standardized eastbound/westbound APIs and northbound APIs need to be developed for different data generating applications for successful integration of network traffic.

3. **Vulnerability of SDN controller:** In any SDN based solution, a compromised network controller can prove disastrous for the network leading to Distributed Denial of Service (DDoS) attack.

4. **Security:** The presence of malicious vehicles and RSUs can lead to routing-based attacks such as blackhole, sinkhole, sybil and replay attacks. Malware attack injection can lead to replication of malicious software on network controllers, routers, switches, vehicles and RSUs leading to tampering of forwarding rules for resource allocation.

1.7.2 Machine learning (ML) for vehicular networks

Presence of big datasets, need for high computing capacity, constantly changing network topologies and channel conditions, and need to serve real-time applications in vehicular networks demands for intelligent learning algorithms that can predict data and network conditions with accuracy and make faster decisions. ML helps to model complex network environments, obtain abstract features, and make appropriate decisions to achieve required QoS for AV [61, 62, 63].

In the vehicular networks, traffic prediction in ML algorithms can help with the following:

1. **Network queuing analysis:** Large scale network queuing analysis helps in uniform understanding of ‘congestion propagation’ among participating nodes and achieve an optimal solution to relieve congestion. There is a need to develop solutions to define congestion threshold, detect queue evolution pattern, congestion control and routing to avoid / overcome congestion.

2. **Analysis of big data transmission dynamics**: This is used to develop solutions to predict routing delays due to big data flows, average link quality

and stability, load balancing over multiple paths and nodes to avoid bottleneck.

3. **ML for SDVN**: The network controller in SDVN can make decisions about resource allocation and configure the network based on the network traffic, congestion and delays. ML can be used to help the network controller make these decisions by studying the traffic patterns. ML integrated with SDVN solutions helps in achieving better network prediction and take timely action.

1.7.3 Vehicular network security

Any network and communication is vulnerable to attacks and needs security. Vehicular networks more so, because of primary use of wireless medium for communication and mobility of vehicular nodes. In a VANET, nodes join and leave the network on the go and carry out V2X communication. Remote communication combined with access to vehicles and their units makes the vehicles more vulnerable to security attacks [64, 65, 66]. In Section 1.6, different threats to vehicular networks and possible attack surfaces are presented. This section discusses the open research issues in the domain of vehicular network security.

Open security issues at different levels of AV: AV security can be broadly segregated into security of processing units, network, gateway and interfaces. Table 4 presents the required possible solutions for open security issues at these levels.

Table 4: Open Security Issues

Issues / Levels	Prevent Access	Detect Attacks	Reduce Impact	Fix Vulnerabilities
Secure Processing	Authentication code, Secure boot	Run-time integrity protection	Resource control, virtualization	
Secure Network	Secure messaging			Secure OTA updates
Secure Gateway	Firewalls, Context aware message filtering	Intrusion Detection Systems (IDS)	Separate functional domains, Isolated Transmission Control Unit (TCU) and On-Board Diagnostics (OBD)	Secure firmware

Secure Interfaces	Machine-to-machine (M2M) authentication Isolation of access points			

Secure processing: The ECUs on in-vehicle network and the gateway nodes need to process messages exchanged among them using different communication protocols. The messages could belong to the critical safety domain as well as not so critical comfort domain. However, one malignant message could corrupt the whole network. To overcome this, solutions are required for secure vehicle data processing that could comprise of secure boot, ECU level message encryption and authentication, key storage and secure OTA software updates. Secure firmware updates with minimal vehicle downtime during update or failed updates may leave the vehicle unusable.

Secure network: Some of the open research issues to attain network communication in AV are context-aware message filtering, message protection through encryption and authentication, network component (ECU, OBU, RSU, gateway) authentication and secure end-to-end connection establishment. The wireless network used for V2X communication too are vulnerable to several attacks as discussed in Section 1.6. Solutions to avoid or overcome these attacks in the highly dynamic vehicular environment is essential, but difficult to achieve.

Secure gateway: Gateway is an essential component of the vehicular network that enables communication between heterogeneous networks using different communication protocols. It provides network isolation and security between functional domains and networks. A compromised gateway module can corrupt the whole network. Hence, a secure gateway is essential. Open research issues for secure network are as important to achieve a secure gateway. A message filter or a firewall solution at the gateway module can isolate the network from malicious data. Gateway should be capable of key storage along with encryption and authentication of messages.

Secure interfaces: An interface is the entry/exit point of the data to/from the network. Components that are used for M2M and V2X communication, telematics, infotainment and diagnostics, if not secured, can leave the entry of malicious data in the network undetected. Hence, it is very important to secure these interfaces. Secure interfaces need to be implemented on a tamper-resistant platform so that they can securely host security applications and their confidential data, thus staying protected against physical attacks. Solutions to achieve secure interfaces need to aim for secure crypto processing, crypto key generation and storage, and secure certificate handling to validate and store information.

1.8 Conclusion:

This chapter presents the significance, applications, related technologies, issues and research avenues in the domain of big data for AVs. The chapter starts with an introduction to vehicular communication (Intra-vehicle and Inter-vehicle communication). Protocols and standards for V2X communication are presented and explained. AV use cases are discussed along with enabling protocols, components and technologies. The big data sources in vehicular networks, rate of data generation, communication and processing are tabulated and discussed, thus highlighting the significance of big data technology in vehicular networks. The chapter presents ongoing research with respect to the technologies involved in big data processing in AV such as data transmission, acquisition, storage, computing, analytics and processing. The highly dynamic nature of vehicular networks presents a major concern for security and privacy on big data in AV. This chapter discusses these security issues and possible solutions. Big data in AV is an emerging field having diverse research avenues. Research directions and open research issues in big data transmission, ML for vehicular networks, vehicular network security are presented with an aim to help the researchers interested in pursuing research in this field.

References

[1] Rakouth, H., Alexander, P., Kosiak, W., Fukushima, M., Ghosh, L., Hedges, C., Kong, H., Kopetzki, S., Siripurapu, R. and Shen, J., 2013. V2X communication technology: Field experience and comparative analysis. In Proceedings of the FISITA 2012 World Automotive Congress (pp. 113-129). Springer, Berlin, Heidelberg.

[2] Sładkowski, A. and Pamuła, W. eds., 2016. Intelligent transportation systems-problems and perspectives (Vol. 303). Springer International Publishing.

[3] Mangel, T., Klemp, O. and Hartenstein, H., 2011. 5.9 GHz inter-vehicle communication at intersections: a validated non-line-of-sight path-loss and fading model. EURASIP Journal on Wireless Communications and Networking, 2011(1), p.182.

[4] Zeadally, S., Hunt, R., Chen, Y.S., Irwin, A. and Hassan, A., 2012. Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems, 50(4), pp.217-241.

[5] Mahmud, S.M. and Alles, S., 2005. In-vehicle network architecture for the next-generation vehicles. *SAE transactions*, pp.466-475.

[6] Khaled, Y., Ducourthial, B. and Shawky, M., 2005, May. IEEE 802.11 performances for inter-vehicle communication networks. In 2005 IEEE 61st Vehicular Technology Conference (Vol. 5, pp. 2925-2929). IEEE

[7] V2V safety communication, Available: https://www.sae.org/standards/

[8] 5G automotive association, Available: https://5gaa.org/

[9] MacHardy, Z., Khan, A., Obana, K. and Iwashina, S., 2018. V2X access technologies: Regulation, research, and remaining challenges. IEEE Communications Surveys & Tutorials, 20(3), pp.1858-1877.

[10] Mohammad, S.A., Rasheed, A. and Qayyum, A., 2011, March. VANET architectures and protocol stacks: a survey. In International Workshop on Communication Technologies for Vehicles (pp. 95-105). Springer, Berlin, Heidelberg.

[11] Kenney, J.B., 2011. Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE, 99(7), pp.1162-1182.

[12] Li, Y.J., 2010, November. An overview of the DSRC/WAVE technology. In International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness (pp. 544-558). Springer, Berlin, Heidelberg.

[13] Gallardo, J.R., Makrakis, D. and Mouftah, H.T., 2010. Mathematical analysis of EDCA's performance on the control channel of an IEEE 802.11 p WAVE vehicular network. EURASIP Journal on Wireless Communications and Networking, 2010(1), p.489527.

[14] van Eenennaam, M., van de Venis, A. and Karagiannis, G., 2012, November. Impact of IEEE 1609.4 channel switching on the IEEE 802.11 p beaconing performance. In 2012 IFIP Wireless Days (pp. 1-8). IEEE.

[15] Weil, T., 2009, November. Service management for ITS using WAVE (1609.3) networking. In 2009 IEEE Globecom Workshops (pp. 1-6). IEEE.

[16] Rabadi, N.M., 2010, November. Implicit certificates support in IEEE 1609 security services for Wireless Access in Vehicular Environment (WAVE). In The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems (IEEE MASS 2010) (pp. 531-537). IEEE.

[17] Park, H., Miloslavov, A., Lee, J., Veeraraghavan, M., Park, B. and Smith, B.L., 2011. Integrated traffic–communication simulation evaluation environment for intellidrive applications using SAE J2735 message sets. Transportation research record, 2243(1), pp.117-126.

[18] Rostami, A., Krishnan, H. and Gruteser, M., 2018, June. V2V safety communication scalability based on the SAE J2945/1 standard. In Proc. ITS Am. Annu. Meeting.

[19] Qu, Q., Li, B., Yang, M., Yan, Z., Yang, A., Deng, D.J. and Chen, K.C., 2019. Survey and performance evaluation of the upcoming next generation wlans standard-ieee 802.11 ax. Mobile Networks and Applications, 24(5), pp.1461-1474.

[20] Papathanassiou, A. and Khoryaev, A., 2017. Cellular V2X as the essential enabler of superior global connected transportation services. IEEE 5G Tech Focus, 1(2), pp.1-2.

[21] Friesen, M.R. and McLeod, R.D., 2015. Bluetooth in intelligent transportation systems: a survey. International Journal of Intelligent Transportation Systems Research, 13(3), pp.143-153.

[22] Prakash, P., Sharma, R., Sindhu, S. and Shankar, T., 2017, December. Visible Light Communication using Solar Panel. In 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT) (pp. 1-5). IEEE.

[23] Winning, A. 2019. Number of automotive ECUs continues to rise. Available: https://www.eenewsautomotive.com/news/number-automotive-ecus-continues-rise

[24] https://www.synopsys.com/automotive/autonomous-driving-levels.html

[25] Daniel, A., Subburathinam, K., Paul, A., Rajkumar, N. and Rho, S., 2017. Big autonomous vehicular data classifications: Towards procuring intelligence in ITS. Vehicular Communications, 9, pp.306-312.

[26] Nelson, P. 2016. Just one autonomous car will use 4,000 GB of data/day. Available: https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html

[27] Lyko, K., Nitzschke, M. and Ngomo, A.C.N., 2016. Big data acquisition. In New Horizons for a Data-Driven Economy (pp. 39-61). Springer, Cham.

[28] Brinkmann, B.H., Bower, M.R., Stengel, K.A., Worrell, G.A. and Stead, M., 2009. Large-scale electrophysiology: acquisition, compression, encryption, and storage of big data. Journal of neuroscience methods, 180(1), pp.185-192.

[29] Cho, W. and Choi, E., 2017. Big data pre-processing methods with vehicle driving data using MapReduce techniques. The Journal of Supercomputing, 73(7), pp.3179-3195.

[30] Fiosina, J., Fiosins, M. and Müller, J.P., 2013. Big data processing and mining for next generation intelligent transportation systems. Jurnal Teknologi, 63(3).

[31] Pandey, M.K. and Subbiah, K., 2016, December. Social networking and big data analytics assisted reliable recommendation system model for internet of vehicles. In International Conference on Internet of Vehicles (pp. 149-163). Springer, Cham.

[32] Guerreiro, G., Figueiras, P., Silva, R., Costa, R. and Jardim-Goncalves, R., 2016, September. An architecture for big data processing on intelligent transportation systems. An application scenario on highway traffic flows. In 2016 IEEE 8th International Conference on Intelligent Systems (IS) (pp. 65-72). IEEE.

[33] Yang, F., Li, J., Lei, T. and Wang, S., 2017. Architecture and key technologies for Internet of Vehicles: a survey. Journal of Communications and Information Networks, 2(2), pp.1-17.

[34] Hu, Z., Zheng, Z., Wang, T., Song, L. and Li, X., 2017. Roadside unit caching: Auction-based storage allocation for multiple content providers. IEEE Transactions on Wireless Communications, 16(10), pp.6321-6334.

[35] Zhang, W., Zhang, Z. and Chao, H.C., 2017. Cooperative fog computing for dealing with big data in the internet of vehicles: Architecture and hierarchical resource management. IEEE Communications Magazine, 55(12), pp.60-67.

[36] Mekki, T., Jabri, I., Rachedi, A. and ben Jemaa, M., 2017. Vehicular cloud networks: Challenges, architectures, and future directions. Vehicular Communications, 9, pp.268-280.

[37] Darwish, T.S. and Bakar, K.A., 2018. Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. IEEE Access, 6, pp.15679-15701.

[38] Al Najada, H. and Mahgoub, I., 2016, December. Anticipation and alert system of congestion and accidents in VANET using Big Data analysis for Intelligent Transportation Systems. In 2016 IEEE Symposium Series on Computational Intelligence (SSCI) (pp. 1-8). IEEE.

[39] Automotive Edge Computing Consortium (AECC), 2020. General principle and vision, white paper. Available: https://aecc.org/wp-content/uploads/2020/03/AECC_White_Paper_v3.0_-_Jan_31_2020.pdf

[40] Thriveni, H.B., Kumar, G.M. and Sharma, R., 2013, April. Performance evaluation of routing protocols in mobile ad-hoc networks with varying node density and node mobility. In 2013 International Conference on Communication Systems and Network Technologies (pp. 252-256). IEEE.

[41] Zhang, C., Ota, K., Jia, J. and Dong, M., 2018. Breaking the blockage for big data transmission: Gigabit road communication in autonomous vehicles. IEEE Communications Magazine, 56(6), pp.152-157.

[42] Sharma, R., Kadambi, G., Vershinin, Y.A. and Mukundan, K.N., 2016. A survey of MAC layer protocols to avoid deafness in wireless networks using directional antenna. In Mobile Computing and Wireless Networks: Concepts, Methodologies, Tools, and Applications (pp. 1758-1797). IGI Global.

[43] Rinki, S., 2014. Simulation studies on effects of dual polarisation and directivity of antennas on the performance of MANETs (Doctoral dissertation, Ph. D. thesis, Coventry University, UK).

[44] Sharma, R., Kadambi, G.R., Vershinin, Y.A. and Mukundan, K.N., 2015, April. Dual Polarised Directional Communication based Medium Access Control Protocol for Performance Enhancement of MANETs. In 2015 Fifth International Conference on Communication Systems and Network Technologies (pp. 185-189). IEEE.

[45] Sharma, R., Kadambi, G.R., Vershinin, Y.A. and Mukundan, K.N., 2015, April. Multipath Routing Protocol to Support Dual Polarised Directional Communication for Performance Enhancement of MANETs. In 2015 Fifth International Conference on Communication Systems and Network Technologies (pp. 258-262). IEEE.

[46] Gopinath, T., Kumar, A.R. and Sharma, R., 2013, April. Performance evaluation of TCP and UDP over wireless ad-hoc networks with varying traffic

loads. In 2013 International Conference on Communication Systems and Network Technologies (pp. 281-285). IEEE.

[47] Huang, Y., McMurran, R., Amor-Segan, M., Dhadyalla, G., Jones, R.P., Bennett, P., Mouzakitis, A. and Kieloch, J., 2010. Development of an automated testing system for vehicle infotainment system. The International Journal of Advanced Manufacturing Technology, 51(1-4), pp.233-246.

[48] Xue, M., Wang, W. and Roy, S., 2014. Security concepts for the dynamics of autonomous vehicle networks. Automatica, 50(3), pp.852-857.

[49] Amoozadeh, M., Raghuramu, A., Chuah, C.N., Ghosal, D., Zhang, H.M., Rowe, J. and Levitt, K., 2015. Security vulnerabilities of connected vehicle streams and their impact on cooperative driving. IEEE Communications Magazine, 53(6), pp.126-132.

[50] Thing, V.L. and Wu, J., 2016, December. Autonomous vehicle security: A taxonomy of attacks and defences. In 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (pp. 164-170). IEEE.

[51] Yu, L., Deng, J., Brooks, R.R. and Yun, S.B., 2015, April. Automobile ecu design to avoid data tampering. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (pp. 1-4).

[52] Mau, D.O., Zhang, Y., Taleb, T. and Chen, M., 2014, May. Vehicular inter-networking via named data-an opnet simulation study. In International Conference on Testbeds and Research Infrastructures (pp. 116-125). Springer, Cham.

[53] Khelifi, H., Luo, S., Nour, B., Moungla, H., Faheem, Y., Hussain, R. and Ksentini, A., 2019. Named data networking in vehicular ad hoc networks: State-of-the-art and challenges. IEEE Communications Surveys & Tutorials.

[54] TalebiFard, P., Leung, V.C., Amadeo, M., Campolo, C. and Molinaro, A., 2015. Information-centric networking for VANETs. In Vehicular ad hoc Networks (pp. 503-524). Springer, Cham.

[55] Xiao, J., Deng, J., Cao, H. and Wu, W., 2016, December. Road segment information based named data networking for vehicular environments. In International Conference on Algorithms and Architectures for Parallel Processing (pp. 245-259). Springer, Cham.

[56] Jain, V., Kushwah, R.S. and Tomar, R.S., 2019. Named Data Network Using Trust Function for Securing Vehicular Ad Hoc Network. In Soft Computing: Theories and Applications (pp. 463-471). Springer, Singapore.

[57] Ananth, M.D. and Sharma, R., 2016, December. Cloud Management using Network Function Virtualization to Reduce CAPEX and OPEX. In 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN) (pp. 43-47). IEEE.

[58] Ananth, M.D. and Sharma, R., 2017, January. Cost and performance analysis of network function virtualization based cloud systems. In 2017 IEEE 7th International Advance Computing Conference (IACC) (pp. 70-74). IEEE.

[59] Sharma, R. and Reddy, H., 2019, December. Effect of Load Balancer on Software-Defined Networking (SDN) based Cloud. In 2019 IEEE 16th India Council International Conference (INDICON) (pp. 1-4). IEEE.

[60] Alioua, A., Senouci, S.M. and Moussaoui, S., 2017, June. dSDiVN: A distributed software-defined networking architecture for infrastructure-less vehicular networks. In International Conference on Innovations for Community Services (pp. 56-67). Springer, Cham.

[61] Taherkhani, N. and Pierre, S., 2016. Centralized and localized data congestion control strategy for vehicular ad hoc networks using a machine learning clustering algorithm. IEEE Transactions on Intelligent Transportation Systems, 17(11), pp.3275-3285.

[62] Grover, J., Prajapati, N.K., Laxmi, V. and Gaur, M.S., 2011, July. Machine learning approach for multiple misbehavior detection in VANET. In International Conference on Advances in Computing and Communications (pp. 644-653). Springer, Berlin, Heidelberg.

[63] Kulkarni, S.A. and Rao, G.R., 2010, August. Vehicular ad hoc network mobility models applied for reinforcement learning routing algorithm. In International Conference on Contemporary Computing (pp. 230-240). Springer, Berlin, Heidelberg.

[64] Xu, L., Yu, X., Wang, H., Dong, X., Liu, Y., Lin, W., Wang, X. and Wang, J., 2019. Physical layer security performance of mobile vehicular networks. Mobile Networks and Applications, pp.1-7.

[65] Moustafa, H., Bourdon, G. and Gourhant, Y., 2006, May. Providing authentication and access control in vehicular network environment. In IFIP International Information Security Conference (pp. 62-73). Springer, Boston, MA.

[66] Franeková, M. and Lüley, P., 2013, October. Security of digital signature schemes for Car-to-Car communications within intelligent transportation systems. In International Conference on Transport Systems Telematics (pp. 258-267). Springer, Berlin, Heidelberg.