# MODELING OF INTERNET OF VEHICLES

*Thesis submitted to the Jawaharlal Nehru University*

*in partial fulfillment of the requirements*

*for the award of the degree of*

**DOCTOR OF PHILOSOPHY**

**IN**

**COMPUTER SCIENCE AND TECHNOLOGY**

**By**

**INTYAZ ALAM**

**SUPERVISOR**

**Dr. SUSHIL KUMAR**


**SCHOOL OF COMPUTER & SYSTEMS SCIENCES**
**JAWAHARLAL NEHRU UNIVERSITY**
**NEW DELHI – 110067, INDIA**

**DEC, 2021**

**SCHOOL OF COMPUTER & SYSTEM SCIENCES**
**जवाहरलाल नेहरू विश्वविद्यालय**
**JAWAHARLAL NEHRU UNIVERSITY**
**NEW DELHI-110067**

# CERTIFICATE

This is to certify that the thesis entitled **"*Modeling of Internet of Vehicles*"**, being submitted by ***Mr. Intyaz Alam*** to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi**, in partial fulfillment of the requirement for the award of the **Degree of Doctor of Philosophy in Computer Science and Technology**, is a bonafide research work carried out by him under the guidance of ***Dr. Sushil Kumar***.

This research work is original and research work embodied in the thesis has not been submitted for the award of any other Degree or Diploma.

24/12/2021
Dr. Sushil Kumar
(Supervisor)
Assistant Professor
SC&SS, JNU
New Delhi-110067

28-12-2021
Prof. T. V. Vijay Kumar
Dean, SC&SS
Jawaharlal Nehru University
New Delhi-110067

SCHOOL OF COMPUTER & SYSTEM SCIENCES
जवाहरलाल नेहरू विश्वविद्यालय
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI-110067

# DECLARATION

This is to certify that the thesis entitled **"*Modeling of Internet of Vehicles*"**, being submitted to the **School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi**, in partial fulfillment of the requirement for the award of the **Degree of Doctor of Philosophy in Computer Science and Technology**, is a bonafide research work carried out by me.

This research work is original and the research work embodied in the thesis has not been submitted for the award of any other Degree or Diploma.

Intyaz Alam.

Intyaz Alam
Ph.D.
Enrolment No. 14/10/MT/010
SC&SS, JNU
New Delhi-110067

# ACKNOWLEDGEMENT

Being a part of this prestigious university in itself is a lifetime opportunity. During Research work for the degree of Ph.D. was a wonderful experience, but it came with a lot of challenges. Though there were some difficulties, new experiences which helped me in the evolution of my personality and career. In the course of work, many people have supported and guided either directly or indirectly which certainly helped me in this journey. Without the support of these worthy people, it would be very difficult to complete my doctoral work smoothly.

Before everyone, I want to thank god for giving me strength and for making my path smooth with fewer obstacles. I would like to express my sincere gratitude to my supervisor Dr. Sushil Kumar for his support in every way possible. His guidance, support, faith and friendly behavior helped a lot during my Ph.D. Your guidance has always inspired me to work hard for completion of my thesis. I, thank you, sir, for everything.

I wish to thank my senior, Dr. Pankaj Kumar Kashyap, for his guidance. I am really grateful for your help, inspiring behavior and time, which motivated and had given me direction during my research work.

I would like to convey my gratitude to Prof T.V.Vijay, Dean of School of Computer and Systems Sciences, administrative staffs, and librarian for ensuring a suitable environment in the school which aided in completing my research work. I would give my sincere thanks to my fellow colleagues, Tayyab Khan, Salam Jayachitra Devi, Indu Dohre, Ankita Jaiswal, Neeraj Pathak, Rinki Rani etc., my juniors, Shariq Anshari, Manoj Kumar, Parveen Kumar, Pinky, Bhawana and Ritesh etc. and seniors Kirshna Kumar, Vipin, Aanchal, Reena, Manisha Rathi etc. for sharing their experiences and knowledge with me and gave their timely support during my research work. I am really thankful for all the help and encouragement.

I want to thank my father, Mr. Mahboob Alam, and mother, Mrs. Asimun Nisha, to whom I want to dedicate my thesis, for helping me at every step. You people are the lights which have

lightened up my path. Without your guidance and support, it would not have been possible. Thank you, father and mother, for trusting me.

Lastly, I also want to thank my brothers, Mr. Muazzam Ali and my sisters, Mrs. Munjera Bano, Rubeena Bano and Nafeesa Bano and sister in laws, Mrs. Quraisha Bano for their love, kindness, and support, which was most important when I used to feel low. I would like to give heartiest thanks to my nephew, Ehan Ali Khan and niece, Muneera Mahboob, for their love.

Thank you, everyone!!

*Intyaz Alam.*

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# LIST OF ALGORITHMS

# ABBREVIATIONS

| Abbreviations | Descriptions |
|---|---|
| IoT | Internet of Things |
| IoV | Internet of Vehicles |
| WSN | Wireless Sensor Network |
| ITS | Intelligent Transport Systems |
| VANET | Vehicular Ad-hoc Networks |
| GPS | Global Positioning System |
| Wi-Fi | Wireless Fidelity |
| C-ITS | Cooperative Intelligent Transportation Systems |
| OAA | Open Automobile Alliance |
| V2R | Vehicle-to-Roadside |
| V2V | Vehicle-to-Vehicle |
| S&A | Sensor and Actuators |
| V2I | Vehicle-to-Infrastructure |
| V2S | Vehicle-to Sensors |
| R&P | Roadside and Personal |
| V2P | Vehicle-to-Personal |
| V2O | Vehicle-to-Office |
| IPv4/IPv6 | Internet Protocol Version 4/ Internet Protocol Version 6 |
| MAN/WAN | Metropolitan Area Network /Wide Area Network |
| LTE | Long Term Evolution |
| 3G/4G/5G/6G | $3^{rd}$ Generations/$4^{th}$ Generation/$5^{th}$ Generation/$6^{th}$ Generation |
| D2D | Device-to-Device |
| ECU | Electrical Control Unit |
| QoS | Quality of Service |
| LCD | Liquid Crystal Display |
| IEEE | Institute of Electrical and Electronics Engineers |

| | |
|---|---|
| IETF | Internet Engineering Task Force |
| CEN | Committee for Standardization |
| W3C | World Wide Web Consortium |
| CCAS | Cooperative Collision Avoidance Systems |
| CAS | Collision Avoidance System |
| MAC | Medium Access Control |
| CA | Collision Avoidance |
| RSU | Road Side Unit |
| SVC | Streaming Over Vehicular |
| CVS-VN | Cooperative Video Streaming over Vehicular Networks |
| AI | Artificial Intelligent |
| DE | Data Engineering |
| NLP | Natural Language Processing |
| ES | Expert System |
| IDM | Intelligent Data Mining |
| FS | Fuzzy System |
| MHA | Meta-heuristic algorithms |
| KD | Knowledge Discovery |
| NIST | National Institute of Standards and Technology |
| WHO | World Health Organization |
| ANFP | Adaptive Neuro-Fuzzy based Payment using Blockchain |
| JA-MVS | Junction-Aware vehicle selection for Multipath Video Streaming |
| SINR | Signal to Interference Plus Noise Ratio |
| DVN | Destination Vehicle Node |
| PLR | Packet Loss Ratio |
| SSIM | Structural Similarity Index |
| E2ED | End-to-End Delay |
| JMSR | Junction-Based Multipath Source Routing |
| 6LoWPAN | IPv6 over Low Power Wireless Personal Area Network |
| OMA-DM | Open Mobile Alliance Device Management |
| CALM-SL | CALM service layer |
| RPL | Routing Protocol for Low Power and Lossy Networks |

| | |
|---|---|
| µIP | micro Internet Protocol |
| ROLL | Routing Overlow Power and Lossy Networks |
| CoAP | Constrained Application Protocol |
| XMPP | Extensible Messaging and Presents Protocol |
| LLAP | Lightweight Local Automation Protocol |
| MQTT | Message Queuing Telemetry Transport |
| HTTP | Hypertext Transfer Protocol |
| HTTP REST | Hypertext Transfer Protocol Representational State Transfer |
| S-MIB | Security Management Information Base |
| OTrP | Open Trust Protocol |
| LoRaWAN | Low Power Wide Area Network |
| S-IC | Security Information Connector |
| HSM | Hardware Security Management |
| AMVT | Adaptive Multipath geographic routing for Video Transmission |
| SDN | Software Defined Network |
| DSRC | Dedicated Short Range Communication |
| CC | Cloud Computing |
| WiMAX | Worldwide Interoperability for Microwave Access |
| D2D-B | Device-to-Device Backhaul applications |
| D2D-C | Device-to-Device Critical application |
| D2D-D | Device-to-Device Direct |
| D2D-N | Device-to-Device Non-critical applications |
| M2M | Machine-to Machine |
| M2M-D | Direct Machine-to Machine |
| CoRe | Collaborative video Retrieval |
| MUPF | Multiple Unicast Path-Forwarding |
| ICN | Information-Centric Networking |
| GP4P | Game-Theory approach for Platoon-centric |
| QoE | Quality of Experience |
| PaFF | Preference-aware Fast Interest Forwarding |
| HPTC | Highly Preferred Content Table |
| ORV | Opportunistic routing solution for pre-recorded Video |

| | |
|---|---|
| ACO | Ant Colony Optimization |
| SNMP | Simple Network Management Protocol |
| QOALITE | QoE-driven and link-quality receiver-based transmission |
| LP | Location Privacy |
| LP-Preserving | Location Privacy-Preserving |
| TPPR | Trust-based and Privacy-Preserving Platoon Recommendation |
| LSTM | Long Short-Term Memory |
| DBN | Deep Belief Nets |
| SOM | Self-Organizing Map |
| MF | Membership Functions |
| FLIS | Fuzzy Logic Inference System |
| ConvNet | Convolution Neural Network |
| 2D/3D | Two Dimension/Three Dimension |
| ReLU | Rectified Linear Units |
| FC | Fully-Connected |
| IBE | Identity-Based Encryption technique |
| PKI | Public Key Infrastructure |
| TPM | Trusted Platform Module |
| TPD | Tamper Proof Device |
| NFV | Next Forwarding Vehicle |
| C-NFV | Candidate Next Forwarding Vehicle |
| HM | Hello Message |
| NIT | Neighbor Information Table |
| SVN | Source Vehicle Node |
| VDR | Vehicle Density of the Road |
| ODVD | Opposite Direction Vehicle Density |
| IDVD | In-Direction Vehicle Density |
| OSM | Open Street Map |
| SUMO | Simulator of Urban Mobility |
| MAC | Medium Access Control |
| OBU | On Board Unit |
| TRH | Tamper Resistant Hardware |

| | |
|---|---|
| DMV | Department of Motor Vehicles |
| RAs | Revocation Authorities |
| LEO | Law Enforcement Organization |
| PARS | Privacy Assure Rewarding System |
| RCC | Reward Collection Centre |
| SoI | Site of Interest |
| PoW | Proof-of-Work |
| PoS | Proof of Stake |
| ECC | Elliptic Curve Cryptography |
| ANFIS | Adaptive Neuro-Fuzzy Inference System |
| ANN | Artificial Neural Network |
| FIS | Fuzzy Inference System |
| RCC | Reward Collection Center |
| PEHT | Pseudonym Exchange History Table |
| $UA_U$ | User Authentication |
| $UA_n$ | User Anonymity |
| $I_n$ | Data Integrity |
| $UC_o$ | Data Confidentiality |
| $P_t$ | Profile Tracing |
| $P_p$ | Privacy Preserved |
| $ID_l$ | ID Linkage |
| $R_w$ | Reward |
| $LC_o$ | Location Confidentiality |
| $ID_d$ | ID Disclose |
| Ex-OR | Exclusive OR |
| OBU | On Board Unit |
| TA | Trusted Authority |
| MNs | Mobile Nodes |
| WAVE | Wireless Access in Vehicular Environment |
| SM | Safety Message |

# LIST OF PUBLICATIONS

## Journals-

1. Alam Intyaz, Kumar Sushil, Kashyap Kumar Pankaj, "A Seven-layered Model Architecture, Network Model, Protocol Stack, Security, Application, Issues and Challenges in Internet of Vehicle", Recent Patents on Engineering, vol. 15, no. 4, ,pp. 116-128, 2021.
2. Alam, Intyaz, and Sushil Kumar. "Functionality, privacy, security and rewarding based on fog assisted cloud computing techniques in Internet of Vehicles." Journal of Discrete Mathematical Sciences and Cryptography, vol. 24, no. 3, pp. 763-775, 2021.
3. Alam Intyaz, Kumar Sushil, Kumar Manoj, Kashyap Kumar Pankaj, "Blockchain Based Intelligent Incentive Enabled Information Sharing Scheme in Future Generation IoV Networks", (Communicated)

## Conferences-

1. Intyaz Alam, Sushil Kumar and Pankaj kumar kashyap "Internet of Vehicle: Layered architecture, network model, security, application, issue and challenges" International Conference on Networks and Cryptology: netcrypt 2019.
2. Intyaz Alam, Sushil Kumar and Manoj Kumar " An Efficient Lightweight Location Privacy Scheme for VANET" International Conference on Networks and Cryptology:netcrypt 2020.
3. Intyaz Alam, Sushil Kumar, Intyaz Alam," An Efficient Lightweight Authentication Scheme for VANETs" IEEE International Conference on Computing. (Communicated)

# ABSTRACT

Internet of Things (IoT) is a world-wide network where smart objects are connected to each other and empowering them to communicate with one another. While considering this smart object as vehicles, IoT can be referred to as Internet of Vehicles (IoV). Thus, IoV is a real-world application of IoT which focuses more on the intelligent incorporation of people, vehicles, and things that exists in the environments. It also provides a platform for Intelligent Transport Systems (ITS) by making vehicles access the information from other vehicles that exist in the environment through the sensors. The access information can be related to drivers, traffic control and pollution control to provide security to the people. IoV focuses mainly on the intelligent integration of vehicles, human, things in the environments. This is larger networks that have the ability to provide services on larger cities including whole country. Additionally, IoV have the capability to acquire, manage and compute the dynamic and large-scale data for vehicles, human, things existing in the environment in order to improve the sustainability, extensibility, computability of the complex network and information system.

Due to the tremendous increased of population; the vehicle owned by the people is also increasing every year. This rapidly increased in the number of vehicles causes more traffic congestion leading to road accidents and increased death toll. Therefore, due to the mobility of the vehicles there is a requirement for better interconnectivity and communication among them. So, the vehicle will be connected to one another through wireless communication using different sorts of gadgets such as cameras, sensors, etc. The devices in the vehicles communicate through internet utilizing wide scope of communication protocol and transmission media. As vehicles are deployed with smart entities such as sensors and provides a communication medium among the vehicles, this becomes a major part of converting the simple transportation mechanism to smart transportation. IoV concepts are mainly used to monitor vehicles and identify the terminals available in the network. These interconnectivity and ability to exchange the information helps to build a new concept in IoT. The communication of the sensors faces a lot of challenging issues. On considering IoV, various challenging issues arise such as sensing complex environment, heterogeneity of

devices, context awareness and connectivity, elimination of redundant data, power, security, guaranteed message delivery, loop-free routing, energy consumption, scalability and mobility. Besides there is other challenging issues in IoV such as location privacy, location accuracy, location verification, vehicle insurance, automobile production, urban traffic management, road infrastructure construction and repair of vehicles critical challenges are to maintain security in information exchanges among the vehicles, inequality in sensors, quality of internet connection, and storage capacity. Besides, employing several vehicles moving on the road as an eye witness to capture the information about the incidents happening on the road is also another challenging task. Privacy is the most important part of IoV since various attacks such as location tracking and identity revealing steal sensitive information to create considerable risk for human lives. The attacker changes confidential information such as speed, direction, path, location of vehicle owner, and exploits its privacy. The existing privacy-preserving schemes like pseudonym schemes, anonymous signing protocol, group signature, and authentication-based schemes, mix zone and silent period, etc. are inefficient in terms of storage, privacy-preserving, and implementation. Furthermore, they impose high overhead and converges very slowly. Lastly, Vehicular communication has attracted reasonable attention recently from both manufacturers and the academic world. This is due to the high demand for on-road safety by road users. Thus, many approaches have been considered for vehicle communication in order to augment the existing on-road safety. One of these approaches is multipath transmission, which supports path diversity and minimizes delay and load balancing, which in turn improves data packet delivery. In multipath video streaming transmission, the selection of the best vehicle for video packet forwarding considering the junction area is a challenging task due to the several diversions in the junction area.

This thesis work aims to address the aforementioned challenges by designing an efficient Junction-Aware vehicle selection for Multipath Video Streaming (JA-MVS) scheme and a novel Adaptive Neuro-Fuzzy based Payment using Blockchain (ANFPB) transportation communication scheme. The JA-MVS scheme considers three different cases in the junction area including the vehicle after the junction, before the junction and inside the junction area, with an evaluation of the vehicle signal strength based on the signal to interference plus noise ratio (SINR), which is based on the multipath data forwarding concept using greedy-based geographic routing. Moreover, we propose a novel ANFPB transportation communication scheme that not only motivates users to take participate in the information sharing problems

with the payment mechanism but also allows users to anonymously share the traffic information with Road Side Units (RSU) in the 5G and Beyond (5G&B) IoV network. Meanwhile, a smart contract is presented to generate pseudonyms to share the traffic information anonymously in a non-trustful 5G&B IoV network. Also, an algorithm ANFPB is presented for the evaluation of payment based on location, timeline, and quality of information shared by the vehicles. In order to achieve these goals; the following objectives were set forth:

- To develop an efficient model on video streaming in urban vehicular environments.
- To provide the An Efficient Lightweight Location Privacy Scheme for VANET.
- To develop an Adaptive Neuro-Fuzzy based Payment scheme using Blockchain to ensure privacy of vehicles in 5G and beyond IoV Networks.

To achieve the first objective, we design a JA-MVS scheme considering the various vehicle positions at the junction area. The multipath transmission considers the junction-aware concept in hop-by-hop transmission. The consideration of road junctions during transmission enhances routing decisions to achieve quality video streaming delivery. In a junction area, the location and direction of the vehicle are essential when the vehicle's signal coverage extends to a junction area, because the selected Next Forwarding Vehicle (NFV) might change its direction of navigation, which could lead to a video packet drop, thereby affecting the quality of the video streaming. Therefore, there is a need to explore the characteristics of the junction area including the vehicles exiting the junction, vehicles at the junction and vehicles before the junction. The vehicles before the junction are considered to be the vehicles at the end of the road, which is at the traffic light. The vehicles at the junction do not have a road-ID but might be in the direction of the Destination Vehicle Node (DVN), while the vehicles after the junction have recently changed their road-ID, navigating towards the direction of the DVN.

To achieve the second objective, we suggested a novel LAP for VANETs in which Trusted Authority (TA) chooses a shared secret key $k$ between $R_j$ and TA, it is stored in the database of TA. We proposed an informal security analysis for authentication, in which we demonstrated that our suggested system meets all VANETs security standards. The proposed method not only integrated authentication, but also keeps the vehicles secret. Furthermore, we simulated and then compared our schemes to other relevant schemes to determine its efficiency and performance. Its provide better performance as compare to the others schemes also comparing our protocol to other relevant protocols reveals that it is more suited to real

world environments. VANETs help in enhancing road safety and optimize traffic flow by transmitting various safety messages among vehicles

To achieve the last objective, we propose a novel scheme ANFPB using blockchain ensuring the privacy of the vehicles, and a further adaptive neuro-fuzzy technique is used to evaluate reward based on location, timeline, and quality of the information shared by the vehicles. Initially, a system model, network model, and block chain technology are presented to define the involved physical entity, fog-cloud network layer for information sharing and to ensure privacy and provides the reward to users respectively in 5G&B IoV network. Then, we briefly define the system initialization process, pseudonyms exchange mechanism for privacy-preserving that include smart contract on blockchain to ensure the authenticity of the vehicles. Then, a novel ANFPB is presented to evaluate the reward for the vehicles based on the shared traffic information. Furthermore, to make the scheme free from fraudulent user's revocation authority revokes the vehicles based on their pseudonym exchange history table.

The above-mentioned works are implemented on the MATLAB (R2016a) and NS-2 environment on Windows 8.1 Pro 64-bit (6.3, Build 9600) platform. The results obtained from the experimental studies show that the proposed works success to out performs the performance of the baseline schemes in terms of packet loss ratio, structural similarity index, end-to-end delay, computation cost and average transaction speed.

# Chapter 1

# Introduction to Internet of Vehicles

## 1.1. Overview

Over the past few decades, the number of the population has been increasing tremendously. Due to this, the vehicle owned by the people is also increasing every year. This rapidly increased in the number of vehicles causes more traffic congestion leading to road accidents and increased death toll [1]. Therefore, due to the mobility of the vehicles there is a requirement for better interconnectivity and communication among them. So, the vehicle will be connected to one another through wireless communication using different sorts of gadgets such as cameras, sensors, etc. The devices in the vehicles communicate through internet utilizing wide scope of communication protocol and transmission media [2]. As vehicles are deployed with smart entities such as sensors and provides a communication medium among the vehicles, this becomes a major part of converting the simple transportation mechanism to smart cities [3]. These interconnectivity and ability to exchange the information helps to build a new concept in Internet of Things (IoT). Figure 1.1 shows the IoT research field and its development areas.

In the research conducted by Raymond James' Industry, it has been reported that the number of devices connected in internet in passed 2011 exceeds the total population on the planet and it has been expecting to reach 50 billion by next year [4]. This excessive increase in the number of connected gadgets provides the entryway for various sorts of automobile to automobile communication which empower universal availability among gadgets there by empowering the IoT world-wide [5].

IoT is a world-wide network where smart objects are connected to each other and empowering them to communicate with one another. When we consider this smart object as vehicles, then IoT can be referred to as Internet of Vehicles (IoV) [6-7].

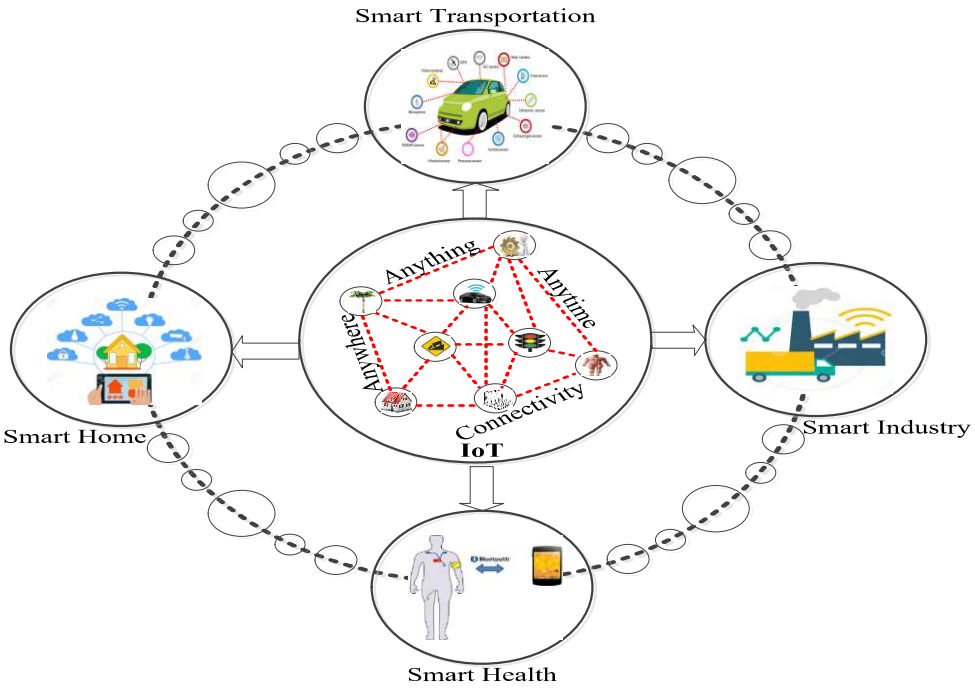



**Fig.1.1** IoT applicable in different research field and its development areas.

Thus, IoV is a real-world application of IoT which focuses more on the intelligent incorporation of people, vehicles, and things that exists in the environments. It also provides a platform for Intelligent Transport Systems (ITS) [8-9] by making vehicles access the information from other vehicles that exist in the environment through the sensors. The access information can be related to drivers, traffic control and pollution control to provide security to the people.

The new generation of IoT navigates the development of conventional Vehicular Ad-hoc Networks (VANET) to IoV. Due to the continuous evolution of communication technologies, IoV attracts large number of leading commercial company as well as researchers. Based on the recent survey it has been predicted that in the near future recent billion things are likely to connect to the internet where vehicle will constitute an important role [9]. There are different obstacles to introduce such types of advancement in large cities. Some of the obstacles are traffic jams, complex road networks, tall buildings, bad driving

condition, etc. Hence, in case of VANET, the devices are unstable, random and temporary. The range of using the device is discrete and local. VANET are not feasible to provide sustainable services or applications for the customers globally. For the past several years, no popular implementation on VANET has been done. Therefore, the usage of VANETs has begun to decline.

IoV is considered to be evolved from VANET [10]. VANET is simply the network comprising of moving vehicles [11]. In this network each moving vehicle is treated as a terminal node and communication is done from one node to another node present in the network. Only the vehicles present within a range of network are able to communicate. When the vehicle moves out of the network range, the communication of the device gets disconnected. This network technology is applicable within a short-range covering only a small area. Therefore, VANETs have a drawback of inability to deal with global information [12]. Further, it has additionally been restricted to operate in areas that have traffic congestions, tall buildings etc. leading to lack of commercial interests. While, IoV can deal with global information by allowing the devices located in a larger range (whole country) to communicate. Due to the accessibility of devices located at large range, it has more commercial interests in comparison to VANETs and also reduces traffic congestion [13]. Hence, IoV is term as the platform for information exchange among the devices in the network in a direct or indirect manner. This implements a secure, safer, efficient, robust and greener environment transportation network.

Unlike VANET, IoV is classified into two main directions for technology such as vehicles intelligence and vehicles networking. The component of vehicles networking includes VANET which is also term as vehicles interconnection, vehicle telematics also known as connected vehicles and mobile internet which is denoted as a wheeled mobile terminal. Similarly, vehicles intelligence is the integration of vehicle and driver. It makes more intelligent due to network technologies such as deep learning, artificial intelligence, swarm computing, cognitive computing, etc. Therefore, IoV is based on the intelligent integration

of vehicles, human, things and surrounding environments. It is a larger network that has the ability to provide services to larger area including whole country.

In the near future, a new concept of Internet of Vehicle would emerge as a new research and development area. This concept has already been initiated and it is in an initial stage in various countries such as in USA, each online device or vehicles are installed with a security chip to define a unique identity of the device in the network [14]. Likewise, in developed part of India, all registered vehicles such as autos, taxi, electronic vehicles, metro rails, government buses etc. have connectivity with Global Positioning System (GPS) and Wireless Fidelity (Wi-Fi) [15]. Meanwhile, European Commission has initiated number of activities for the up-liftment of next generation Cooperative Intelligent Transportation Systems (C-ITS) [16]. The study of various reports recommends that there is a positive feedback regarding the "connected vehicles" from various countries such as Australia, UK and USA [17]. Several international companies are working on this area to developed new innovative ideas. Google Company is collaborating with leading Information Technology (IT) and automobile companies in order to developed Android based system for connected drive under the association Open Automobile Alliance (OAA) [18].

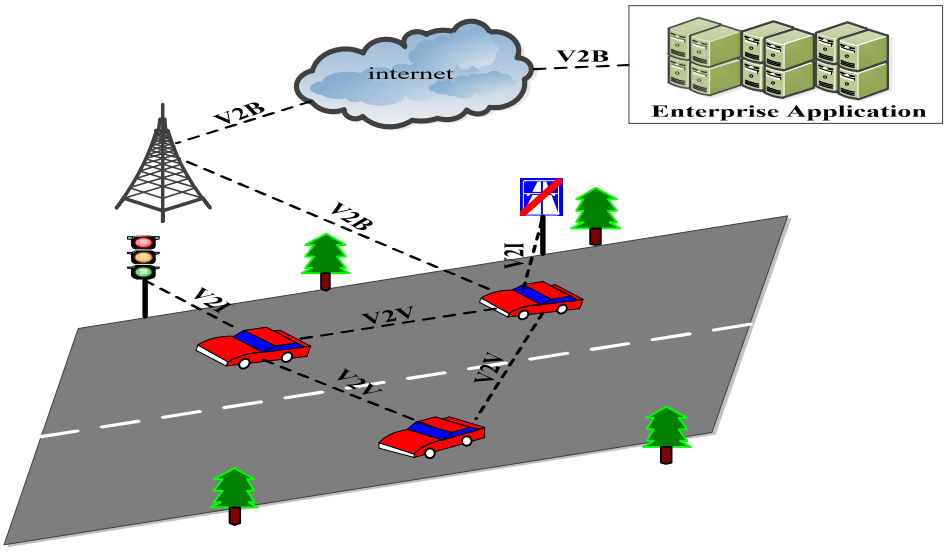



**Fig.1.2** General Architecture of IoV.

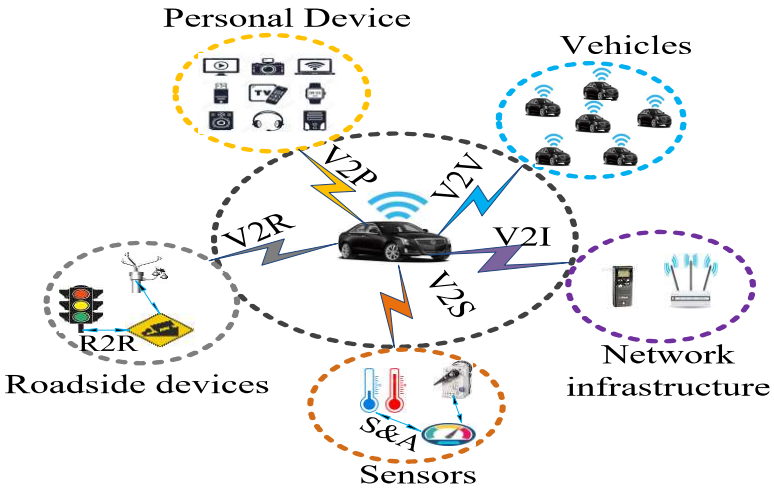
On the other hand, Apple Company has introduced a system "CarPlay" which provides all the services of iPhone to the driver through car display along with voice support feature [19].

Even though IoV is a new emerging area of research, several countries have already started applying the concept of IoV. In the coming generation lots of development in IoV can be conducted as it has scope of exploring and applicable on real time basis. In present scenario, USA is the country that has already deployed IoV concept in all the devices connected in the network by installing a security chip. IoV concepts are mainly used to monitor vehicles and identify the terminals available in the network. Similarly, India is also another country that deployed the concept of IoV. In the capital city of India, all the vehicles that have registered are allowed to set up GPS to track the vehicle's location [17]. Meanwhile, European Commission has taken up several initiatives for the betterment of ITS [20].

The heterogeneous network architecture of IoV [21] includes seven types of vehicular communications. The types include Vehicle-to-Roadside (V2R) unit, Vehicle-to-Vehicle (V2V), Sensor and Actuators (S&A), Vehicle-to-Infrastructure (V2I) of mobile networks, Vehicle-to Sensors (V2S), Roadside and Personal (R&P) Device, Vehicle-to-Personal (V2P) devices are shown in Figure 1.3. Here, interaction among different IoV elements leads to vehicles information exchange at multi-level by providing awareness to the vehicles, and this also provides passengers and motorists with valuable information for secure traveling. The elements taking part in the IoV environment can be an object, devices, etc., which interact with each other to exchange the information. The communication among these elements involves the collection of information, exchanging, storing and analyzing the information to make decisions by less human interventions.

Generally, the applications of IoV are classified into two major categories such as User applications and Safety applications. User applications provide value added services to the user. Whereas, the applications that provide safety of the vehicle along with safety of the passengers travelling on roads by giving notification about any dangerous situation of the

vehicles. On considering IoV various challenging issues arise such as sensing complex environment, heterogeneity of devices, context awareness and connectivity, elimination of redundant data, power, security, guaranteed message delivery, loop-free routing, energy consumption, scalability and mobility. Besides there are other challenging issues in Internet of Vehicle such as location privacy, location accuracy, location verification, vehicle insurance, automobile production, urban traffic management, road infrastructure construction and repair [21-22].




V2V: Vehicle-to-Vehicle, V2I: Vehicle-to-Infrastructure
V2S: Vehicle-to-Sensors, V2R: Vehicle-to-Roadside Unit
V2P: Vehicle-to-Personal Device, R2R: Roadside-to-Roadside
S&A: Sensor-and-Actuator, R&P: Roadside and Personal device

**Fig.1.3** Types of vehicular communications in IoV.

The following is the chapter's explanation. Section 1.1 gives a brief overview of the IoV. Section 1.2 describes briefly about different architecture of IoV. Section 1.3 describes the case study of IoV architecture in real life scenario. Section 1.4 explains the standards of protocols which are used in IoV architecture. In section 1.5 explain about the characteristics of IoV. Section 1.6 explains the various applications of IoV. Section 1.7 discusses the challenges faced by the IoV network. Section 1.8 explains the various securities of IoV

networks. Section 1.9 presents the motivation behind the research and explains the significance of the work by defining the importance of the proposed work. The problem statement is explained in section 1.10 which is followed by the objectives and the proposed methodology for achieving the said objectives, respectively. The last section of chapter presents the layout of the thesis.

## 1.2 General IoV Architectures

The greatest challenges of IoV is the ability to integrate multiple components such as sensors, vehicles, roadside communication infrastructures, human and personal devices in order to provide comfort, safety and better traffic condition levels. This function requires the setting up of requirements and several functionalities to encapsulate as a new layer in layered IoV architecture [18]. The most important challenging issues in layered design architecture are the most favorable number of layers and the efficiency of each layer. Some of the challenging issues are [23]:

- Characteristics of network that includes scalability, interoperability, modularity, reliability among other devices in the network.
- Communication technologies that includes Bluetooth, Wi-Fi, 4G/LTE, Zigbee, etc.
- Data security includes integrity, confidentiality, authentication, availability, and identification.
- User interaction includes audio, visual, and haptic.

In this regard, the authors also recognized numerous issues that are necessary to considered while designing IoV architecture [24]. Some of the issues are taken into consideration such as interconnection of devices in the heterogeneous networks, internet integration, adaptation to new technologies, service-oriented architecture involving plug and play based interface.

After considering these issues the author developed a framework focuses on the network, interaction and environment model. This framework involved layered architecture that

provides seamless integration of inter-device communication in the IoV system [25]. In this framework some basic information of the layers are defined below.

### 1.2.1 Interaction Model in IoV

There are six main components involved in IoV ecosystem such as Person, Vehicle, Personal Device, Sensing Device, Network Infrastructure, and Roadside Device. These components interact with each other in IoV network. In case of vehicle, all nearby vehicles are communicated through a communication link established among them to exchange the information such as alerts signal, traffic condition, physical variables, etc.[26], In case of IoV, person, people that request to access for network services in environment are considered. In case of personal device, a device that belongs to individual person for accessing to the network service in the IoV environment is considered. All the devices that are involved in the network for sharing data are considered in network infrastructure. The Sensing device like sensors and actuators are used for collecting data or information about the parameters of vehicles such as fuel consumption, tire pressure, vehicle temperature, etc. Similarly, it can collect information of person's health levels such as blood pressure, blood oxygen level, heart beat rate, etc., and it can also collect environmental information such as pollution level, weather condition, noise level, etc. Lastly, the device used in the transportation system infrastructure are known as road side unit and it includes devices such as traffic lights, radars that capture the relevant information about accidents, traffic condition, etc. The interaction that happens among the various IoV elements leads to multi-level exchange of data such as Device to device, Vehicle to vehicle, Vehicle to device, person to device and person to vehicle [27]. This helps to provide vehicle information in order to enhance the situational awareness of the vehicles and avail the information about the travel environment to the passengers or driver.

All the components present in the IoV environment such as sensors, actuators, vehicles, personal devices etc. are represented as devices or objects that communicates with each other. The Device-to-device (D2D) interaction in IoT [28-29] has become an essential part

and further extends to include other types of interaction. This type of interaction in IoV environment involved several devices for communication purpose, data collection, exchanging information, storing and analyzing data and makes decision without involving human interventions.

### 1.2.2 Environmental Model

In case of environmental model, the communication outside the vehicle is describes that enables the interactions of multiple devices, and vehicles in the network [21].Both these devices function together to provide improved services in terms of comfort, safety, and reduction in traffic congestion by deploying vehicle to vehicle, vehicle to roadside unit, vehicle to personal device, roadside unit to personal device interactions [30-32].

### 1.2.3 Network Model

The network model of IoV is designed in this section, consisting of different components of the network.

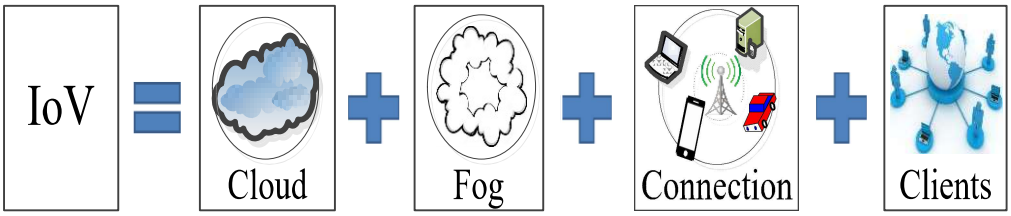



**Fig.1.4** Four network elements of IoV.

The components in the network play a significant role in expressing the functionalities of the IoV in a heterogeneous manner. The design of the network model consists of four types of components such as cloud, fog, connection, and clients. The combination of the components to form a network model is shown in Figure 1.4. The details of the network model including all the elements inside each component are shown in Figure 1.5. The `Cloud' is the major component that is used to store all the information of the IoV. Several services such as information processing, intelligence computing are the essential services offered on the

cloud platform with the help of cloud infrastructure. In IoV, the data collected from various devices are huge due to the tremendous increase in vehicular applications. The increase in the amount of data, finds it difficult to enhance the services related to vehicles. So, the network model which depends only on the cloud to store and processed the information fall short. Hence, the fog component is introduced to improve information processing and storage. Fog acts as an intermediary between the cloud and the devices.

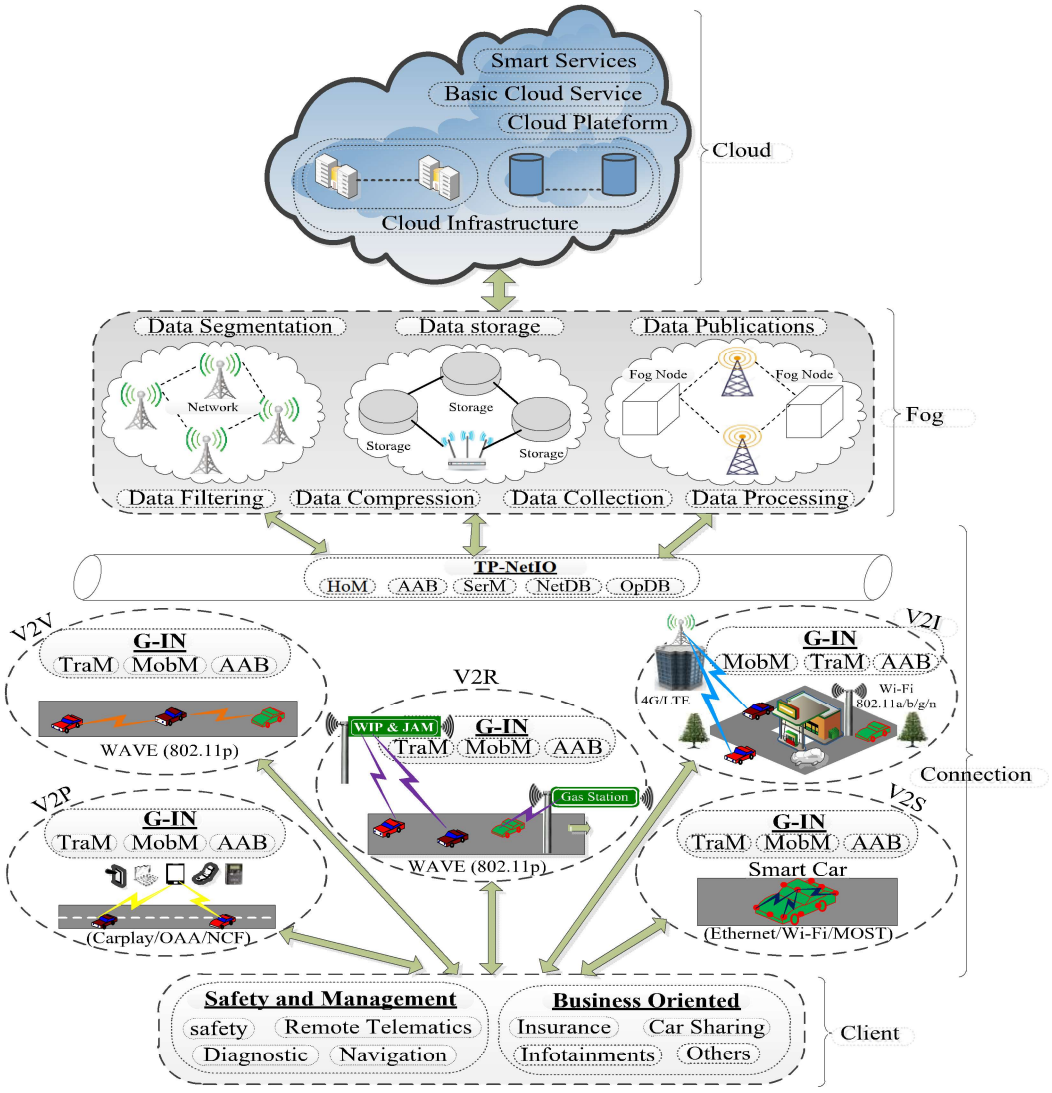



**Fig.1.5** Network model of IoV with four network elements.

In addition, fog component has various advantages such as safe storage of the cloud, save bandwidth and reduces the latency, etc. Fog consists of fog nodes which can be a mobile and it supports mobility. The nodes can join or leave the network. The information is processed in the Fog before it sent it to the cloud. Services are accessible on the cloud through Fog only with the help of connection. The connection is the third component of the IoV network model. Different types of wireless technologies have been exploited to perform different types of vehicular communications. Finally, all the connections are deployed by the client-side application, which is nothing but the last component in the network model. Client-side application services may differ from one client to another client. So, a priority is assigned to the types of wireless technologies applicable to various client-side applications.

### 1.2.4 Propose Layered IoV Architecture

The most significant challenges overcome by IoV is their consistency in the integration of various devices such as sensors, actuators, vehicles, camera, humans, etc. to enhance the levels of safety, security, comfort and traffic congestion levels. In the case of layered architecture, the main challenge is to maintain an optimal number of layers and provide their functionalities of each layer. Functionality can be classified as:

- According to the characteristics of network including scalability, reliability, interoperability, and modularity
- According to the technologies used for communication purposes such as Bluetooth, Wi-Fi, 4G etc.
- Based on data security such as authentication, integrity, confidentiality, availability, etc.
- Based on interaction among the user, it may be audio, visual, and haptic.

The main objective of IoV architecture is to have secure integration among the devices on the internet. The integration can be among multiple vehicles, things, networks, etc. to

maintain the best communication effectiveness that is operational, controllable, and manageable.

#### 1.2.4.1 User Interface Layer

In this layer connection with the drivers is done directly through the administration interface to manage the notifications from the driver and provide the best solution from the present scenario to reduce the driver's disturbance. Suppose that if a car is likely to meet collision, ahead of that set of lights or signals can get activated to provide alertness to the driver. In this layer, vehicle communication is done based on two communication systems, such as a system based on information and system based on control. In this system, based on information, all the relevant information, including information of the route, information of traffic, car parking information, warning of risks for any components of the environment such as vehicle or driver. Some start-up companies have been focusing on IoV development. An example of Google Company and other car manufacturing company which developed an Android platform known as the Open Automotive Alliance to provide reality to the connected car. A system based on control records all the changes done while driving, certain elements related to driving, includes collision avoidance, control speed, lane keeping, etc.

#### 1.2.4.2 Data Acquisition Layer

This layer is responsible for collecting information from devices install on roads by using various internal sensors of the vehicle, data gather sensors, traffic signals, data captured from the communication of the vehicle. Various schemes for data collection have been proposed, which are based on road division into groups of clusters along with cluster head. Data can also be collected dynamically based on the mobility of the vehicles and changes in the network topology. Data transmission based on interaction is classified as intra vehicular transmission and inter-vehicular transmission. Intra vehicular transmission focuses on data collected from sensors to a central device that is located inside the vehicle connected through a wireless or wired network. We assumed to have 200 sensors per vehicle in the

coming years. The topology of the sensors networks is stationary as a sensor does not change the position.

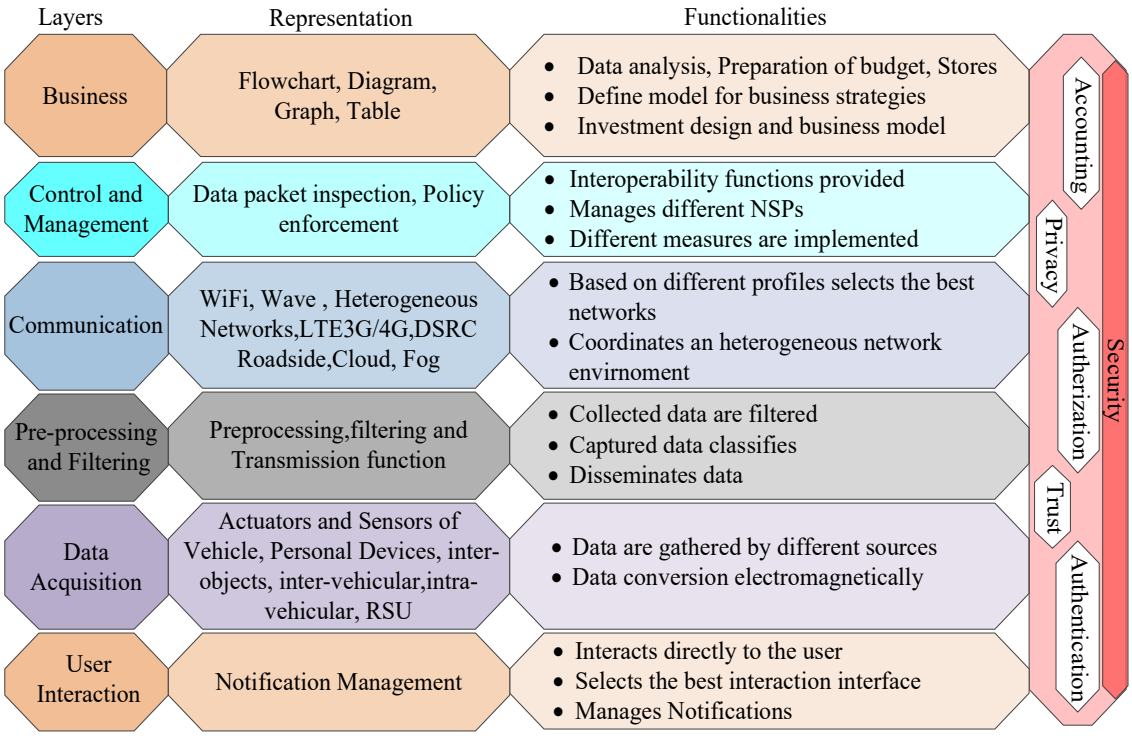



**Fig.1.6** Seven layered architecture of IoV.

Hence, sensors which are located inside the vehicle do not have any energy limitation as the sensors are connected to the power systems of the vehicle. The information collected from the sensors is stored in the Electrical Control Unit (ECU). Later, this information is used in the execution of several tasks related to the vehicle. In addition, the transmission of data requires a high-security level, high reliability, and low latency in order to protect the control systems of the vehicle.

In IoV, data acquisition in an intra-vehicle network is an emerging research area. In the Inter-vehicular network, data transmissions and communication are carried out with the external entities, including devices, vehicles, sensors, etc., of the IoV environment. The process of information exchange is done in real-time to provide safety.

#### 1.2.4.3 Data Pre-processing and Filtering Layer

In this layer, the analysis of the already collected information is done. This analysis helps to filter the irrelevant data from the transmission, leading to a reduction in network traffic. The decision of transmission is entirely based on the service profile of the vehicle, which is an inactive state. Various approaches to data filtering have been proposed. Despite this, the novel data mining technique is needed to extract data efficiently, accurately and quickly.

#### 1.2.4.4 Communication Layer

The most suitable network to send the information is selected in this layer by considering different parameters. Quality of Service (QoS) and congestion level available for different networks, information related to privacy and security, etc. are some of the parameters that can be deal with. Every communication network has its own aspects. Networks should be incorporated in a manner to such an extent that the environment gives connectivity and consistent services alongside the ideal quality to the clients on the basis of several parameters, including the location of the device, access technologies available for the client's gadget, etc. The main challenge for this layer is planning a wise approach that chooses the most appropriate network utilizing the applicable data.

#### 1.2.4.5 Control and Management Layer

Management of network service providers present in the IoV environment is done this layer. Not only the management of the network service provider but the management of the information is also done in this layer using various techniques such as traffic management, packet inspection, and traffic engineering. The primary function of this layer is the management of data exchange among the different services.

#### 1.2.4.6 Business Layer

The main purpose of this layer is to properly plan for the advancement in business models depending on application utilization of information and statistical investigation of the

information. In this layer, a large amount of information is processed using the cloud computing technique. The information, which has already processed, is given to various data service providers to implement a new application.

This processed information is also used by various government sectors for future development purposes. Different analysis tools such as use case diagram, flowchart, graphs, tables, etc. are used in this layer. Besides all the features, this layer is also responsible for storing; analyzing the information, decision making of the resources to be used in financial investment, budget estimation for management operation, and data management.

#### 1.2.4.7 Security Layer

This layer is given in vertical alignment in Figure 1.6 to indicate direct communication to all the layers in the architecture. With the help of this layer, all the security operations such as authentication, integrity, confidentiality, availability, access control, etc. are supported to provide a secure IoV environment. This layer is the solution to various cyber-crimes in IoV.

## 1.3 Case Study of Proposed IoV Architecture

This case study explains how the different layers of IoV architecture worked together, as shown in Figure 1.7. Let us assume that there is a vehicle having an internal problem in the IoV ecosystem such as a short circuit in the engine.

**(1)** First, in the acquisition layer vehicle, try to detect the problem through multiple internal sensors of the vehicle by analyzing the performance of the system. The problem can be either internal or external causes of other vehicles. Such as electromagnetic signals emitted by other vehicles in range causes malfunction the other vehicles or roadside sensors affect the vehicle's performance. The ECU catches the problem that has arises either by an internal or external cause.

**(2)** The ECU unit notifies the problem of the vehicle to the Driver by selecting the best possible display element (e.g. LCD panel) or event (e.g. audio or haptic) depending upon the

current situation. For example, if the ECU unit detects problem either collision would be happening with a vehicle ahead of him with current speed then alert signal (notification RED light on activated on vehicle dashboard) or engine is too much-heated cause of continuous running, then message appears to stop the vehicle and use coolant to cool down the engine otherwise engine may be blast.

**(3)** In the pre-processing layer, the ECU unit filters the information, reduces the information size by removing the irrelevant information; thereafter, it categorizes in two different types, either mechanical or environmental. The information is now transmitted to the nearby vehicles or roadside hoardings.

**(4)** The best possible access network is selected for data broadcasting in a periodic manner. The selection of networks depends on several parameters such as vehicle profile subscribes for which network, quality of service provided by the network, congestion ratio etc. The transmitted information (i.e. data or packet) must be protected by external attacks. Security layer prevents from cyber-attacks and also provides extra data integrity, authentication, and confidentiality to the packet.

**(5)** After selection of the best technology, network data is circulated by the problematic vehicle to the nearby vehicles (external to malfunctioned vehicle) in the pre-processing layer.

**(6)** The nearby vehicles which receive the information about the malfunctioned vehicle, their ECU unit notify the driver through any notification element, audio/video, or through the vibration of sensors.

**(7)** Also, The ECU of receiving vehicles identify and try to rectify the problem such as, display the reduce the current speed to avoid collision with the malfunctioned vehicle ahead or avoid the congested roads by showing the alternate route on GPS in the pre-processing layer.

**(8)** Control and management layer responsible for forwarding the information to other vehicles in the IoV ecosystem, such as displaying the message in roadside hoarding about there is malfunctioned car is stopped ahead of the road, congestion in the road. This layer also provides a solution to the problem such as deployment and displaying another route option to avoid congestion, manipulate the traffic light signals so that overall traffic conditions would be better.

**(9)** These information and roadside infrastructure are stored in cloud services either remotely or locally. This information is further processed to service, improve the existing IoV ecosystem, and developed future infrastructure.

**(10)** Now, the malfunctioned vehicle starts the analysis of the current situation and sends the gathered information to the vehicle manufactured company and decides whether isolate the damaged part of the vehicle to avoid further damaged such as the explosion of the engine or short circuit.

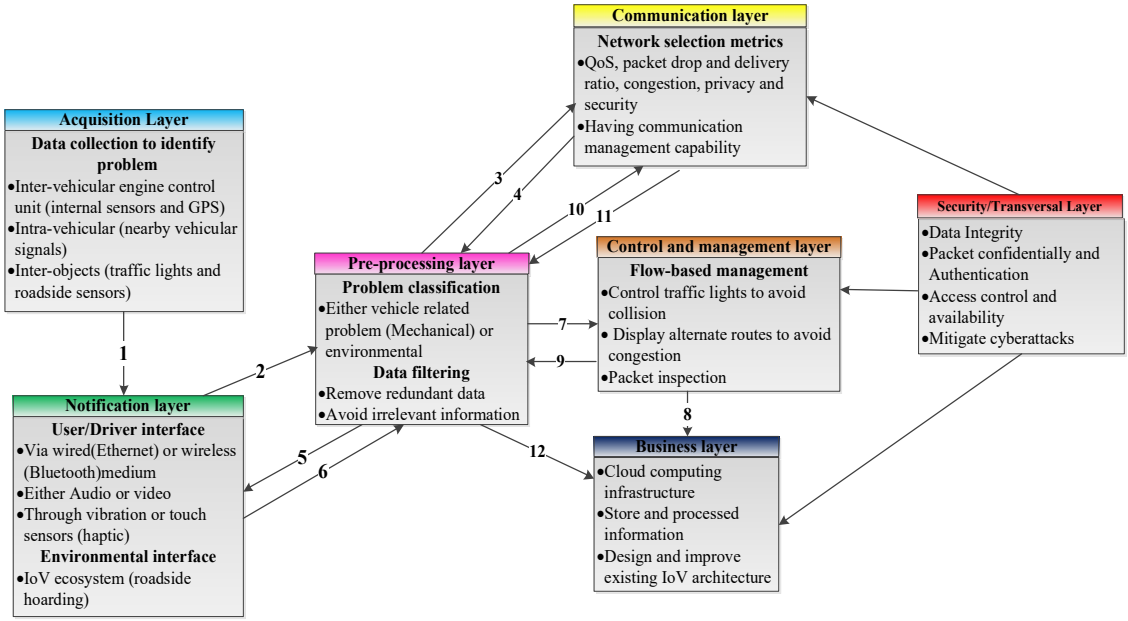



**Fig.1.7** Sequence diagram for an IoV scenario.

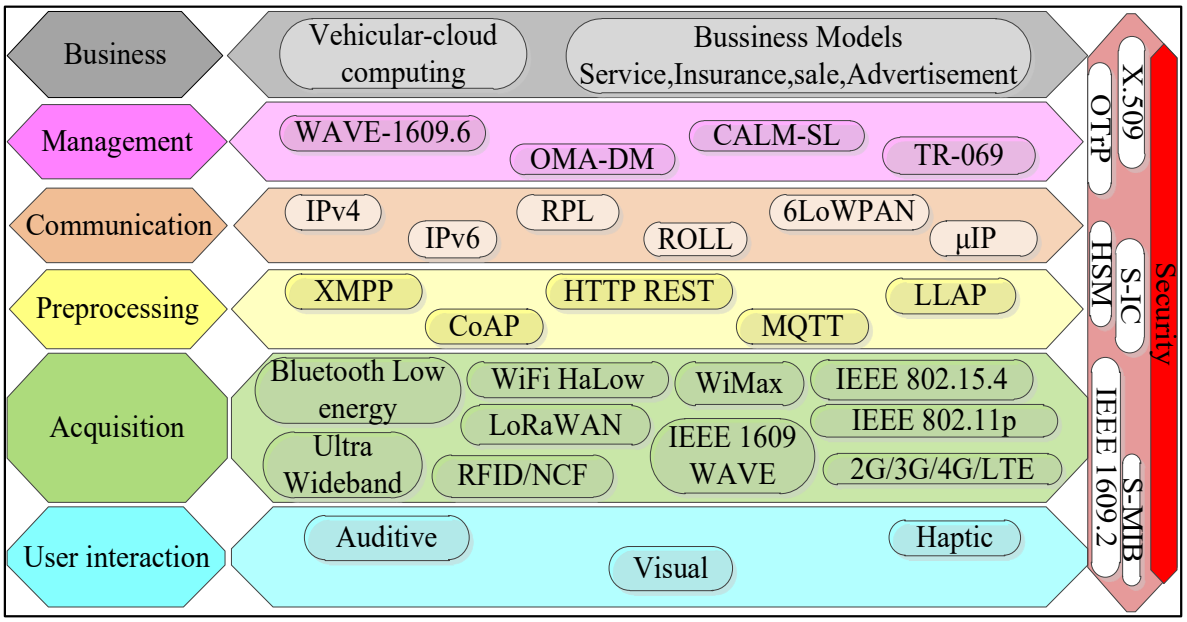
**(11)** This information is sent out by vehicle using an appropriate network based upon vehicle company profile, occupant profile, cost and volume of information). All this information is in encrypted form as it includes personal information (body temperature, anxiety & stress level determined by wireless body area network sensors) of the customer along with their vehicle status. So all these communications are protected by the security layer.

**(12)** In the business layer, a detailed personalized report is prepared and stored into the cloud-related to malfunctioned vehicle. This information is further used to determine the cause of failure and also tackle the same problem if it again occurs into another vehicle of the same model in the future. Thus by follow-up, these report cards in the future repair cost of the damaged vehicle would be reduced. Finally, the vehicle manufactured company notifies the driver about the type and level of the damaged part of the system. They also investigate the time duration of a specialized mechanic or towing machine to arrive and whether the damaged part is in the condition of repair or replacement with one in the Service Centre — all these communications from the client to the business support layer.

## 1.4 Standards Protocols for IoV

IoV includes numerous actors, and the connectivity among these actors must be guaranteed. The most fundamental issues in interconnecting the vehicles are interoperability. Therefore, to fulfill this issue, a standards IoV framework is needed to develop. Meanwhile, lots of work has been carried out to define the standards and protocols for IoV.

Several international organizations such as the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), the European Committee for Standardization (CEN), EPC global, etc., which is governed by the World Wide Web Consortium (W3C), are working on the standardization for IoV and development of protocols related to IoV. These organizations focused on the standards assigned to the application developers by providing accurate access to the data acquired from the vehicles.




6LoWPAN=IPv6 over Low Power Wireless Personal Area Network
OMA-DM=Open Mobile Alliance Device Management
CALM-SL=CALM service layer
RPL=Routing Protocol for Low Power and Lossy Networks
µIP=micro Internet Protocol
ROLL=Routing Overlow Power and Lossy Networks
CoAP=Constrained Application Protocol
XMPP= Extensible Messaging and Presents Protocol
LLAP= Lightweight Local Automation Protocol
MQTT= Message Queuing Telemetry Transport
HTTP REST= Hypertext Transfer Protocol Representational State Transfer
S-MIB= Security Management Information Base
OTrP= Open Trust Protocol
LoRaWAN= Low Power Wide Area Network
S-IC= Security Information Connector
HSM= Hardware Security Management

**Fig.1.8** Protocol stack for IoV.

The data related to the vehicle include personal information, vehicle identification, speed and acceleration, battery status, the pressure of the tire, etc. Among the several organizations, ETSI and CEN developed the standards to ensure interoperable connectivity among the vehicles that are manufactured from a different company. This basic set of standards was developed at the request of the European Commission. In Figure 1.8 above, some of the prominent protocols determine by various Organizations of the international standardizations have been shown. The application layer also is implemented for IoV platform also.

## 1.5 Characteristics of IoV [22, 33-34]

In vehicular networks, the nodes are represented by vehicle that has different behavior in comparison to other wireless nodes. Hence the vehicular network consists of numerous qualities that may influence the design of IoV technologies. Out of all the characteristics some of them may behave as a challenging task in IoV technological development. While some other may bring benefit to the environment.

### 1.5.1 Highly Dynamic Topology

In vehicular network, vehicles are move continuously at high speed in comparison to mobile nodes. The continuous movement of vehicle causes the topology of the network to frequently change. Therefore, in IoV development such dynamic nature of the network topology must be considered carefully.

### 1.5.2 Variable Network Density

The density of the network varies in IoV according to the density of traffic. The network density is very high in case of traffic jam whereas it is very low in case of suburban traffic. In both the cases, the network may disconnect frequently.

### 1.5.3 Huge Size Network

The size of the network is large in dense and urban areas such as city areas, entrance of big cities and highways.

### 1.5.4 Geographical Communication

The communication in Vehicular networks is different in comparison to other networks. In other networks, Unicast or Multicast mode of communication is carried out where the endpoints have unique ID or group ID. Whereas, in vehicular networks a different type of communication is used addressing the geographical areas for forwarding the packets.

### 1.5.5 Predictability of Mobility

In comparison to mobile ad-hoc networks, Vehicular networks have different mobility. In mobile Ad-hoc networks the nodes or terminal moves in a random manner, whereas the movement of vehicles is constrained on the topology of the road and layout. Additionally, the vehicles movement depends on the traffic lights, road signs and based on other moving vehicles that lead to predict based on the mobility.

### 1.5.6 Sufficient Storage and Energy

In case of vehicular networks, the common characteristics of nodes is that they have sufficient energy and computational power of storage and processing. As the nodes in this network are cars or vehicle rather than handheld devices.

### 1.5.7 Several Communicating Environments

Vehicular networks are operable at two types of communicating environments such as highway traffic and city traffic conditions. The environment in highway traffic condition is relatively straightforward and simple. Whereas, traffic in city condition becomes more complex. These are because in city, the streets are often separated by trees, buildings and other obstacles. Hence, no direct line of communication is available in the direction of any intended data exchange.

## 1.6 Applications of IoV

IoV has a wide range of uses. We divide them into three major categories based on their uses which are shown in the Figure 1.9 below.

### 1.6.1 Safety Driving

The applications related to safety driving are referred to as Cooperative Collision Avoidance Systems (CCAS) [35]. This has been further extended to Collision Avoidance System (CAS)

and allowed to share the CAS information among the nearby vehicles through V2V communication system [36-37]. CAS provides various functionality such as sensors or radar is used to detect an imminent crash, provides warning to the driver at right time so that immediate brake can be applied. Therefore, CAS is also known as collision mitigation or collision warning system, it is also known as pre-crash system.

CarTALK 2000 was developed in [38] and it involves CCAS. Algorithms were developed to test and assist the driver. A special congestion control policy along with redundant detection mechanism for providing emergency warning messages was developed by Yang et. al. in order to achieve low communication and delay cost. Another author developed a risk-aware Medium Access Control (MAC) protocol for Collision Avoidance (CA) [39-40] purpose. For each vehicle the medium access delay is set for emergency and vehicles which are in emergency situation can disseminate warning signals with less delay in order to reduce chain collisions. Meanwhile, another author also proposed V2R [41] based vehicle control system. An algorithm based on fuzzy is responsible for safety of vehicle's and avoids collision. Further, an algorithm for collision judgment was developed by [42] for estimating relative positions and determined the potential collision areas to reduce the unnecessary and false warnings system.

## 1.6.2 Efficient Transportation

In transportation management, efficiency is the most important factor. Vehicular network brings additional opportunities for efficiency improvement. Efficient transportation applications are categorized as route navigation, parking navigation, intersection control and cooperative driving.

### 1.6.2.1 Route Navigation

Navigation of Vehicular network is studied in order to overcome the difficulties of GPS or other similar navigation systems. In [43], the authors proposed a navigation route considering the information of real time traffic condition and the consumption of fuel.

Another author developed a route selection algorithm that has the ability to deal with traffic congestion optimizing the utility of road. The algorithm VSPN [44] is developed mainly for privacy preserving navigation system that uses the data of road conditions collected through Road Side Units (RSUs) and speed data to guide the vehicles. In paper [45-46], Leontiadis et al. developed a crowd sourcing traffic information based system in an ad-hoc manner.

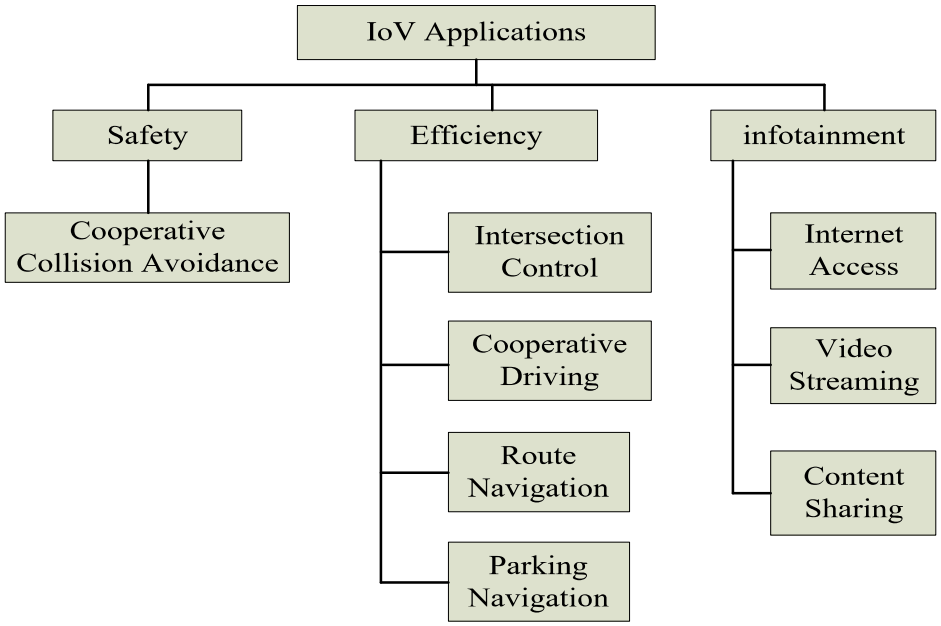



**Fig.1.9** IoV applications.

### 1.6.2.2 Parking Navigation

Vehicular networks can help in finding available space for parking [47]. In [48], the author formulated the problem based on travelling salesman problem varying time, and developed a model for computing the best route that a vehicle can traverse visiting all spaces available for parking.

### 1.6.2.3 Intersection Control

Controlling traffic at intersections is a key issue for ITS. The main problem is scheduling of traffic signals efficiently based on the information volume of traffic in order to improve

fairness and reduce the time of waiting. There are several existing intelligent intersection control algorithms, and it has been categorized as traffic light scheduling and Non-traffic light scheduling.

Most of the intersection control is based on traffic light where the main issue is the determination of good signal scheduling plan. Earlier, road detectors were used to capture traffic volume information. The traffic signal plan changes constantly in order to adapt to the changing traffic conditions. Traffic light scheduling is considered as a new stage of intersection control system. The detailed information of the vehicle such as ID, position, speed is determining using V2V or V2I communication [49-50]. Therefore, more efficient and accurate scheduling can be obtained.

In [51], V2V based traffic light control system is presented. The system leads to reduction of communication cost through the clustering approach of vehicles for intersection. The cluster density of the vehicles is determined by clustering algorithm and transfer to the traffic signal controls for setting the time cycle.

V2I based traffic light control system is also studied widely. In paper [52-53], the author used a controller node to collect the queue length information as well as proper cycle time of the traffic signal using Webster formula. Meanwhile, priority of the vehicles is also considered in another paper [54] and scheduling of traffic signal is done with quality of service provisioning. There are some other works where signal scheduling is designed based on combinatorial optimization problem to determine an optimal scheduling traffic signal plan. For solving such problems, there are several methods that can be applied such as branch and bound [55], dynamic programming [56-57] and linear programming [58]. Besides some researchers also used other intelligent algorithms based on fuzzy logic [59] and Q-learning [60-61].

Non traffic light intersection control approaches were also available. In algorithms based on maneuver manipulation, the driving pattern of the vehicles are controlled completely by the intersection controller that calculates the most appropriate trajectories of individual vehicles

in order to provide safety path of the vehicle without causing collision [62-64]. The accurate calculation of speed and position of the vehicle is needed that increased the complexity. Additionally, unlike maneuver there is non-traffic light involved in vehicle scheduling algorithms that schedule for creating permissions to pass through intersection instead of focusing on driving behaviors.

In the papers [65-66], a reservation based intersection control system was developed that provides facility to the vehicles to interact through wireless communication with an intersection controller to reserve for passing. Based on the condition of traffic and reservations, the intersection controller takes the decision to accept the request or reject. Another author also proposed a mutual exclusion model to realize the scheduling of the vehicle with no traffic light.

### 1.6.2.4 Cooperative Driving

This technology coordinates a queue of vehicles in order to make them drive as a single vehicle. This improves the efficiency and energy. In paper [67], the author designed a practical result of longitudinal control for platooning truck. According to the measurement of distance among the vehicles, a robust platoon controller was designed and developed using sliding mode control. In [68], the author examined the error gain from disturbance for the platoon scales along with the vehicles number. In [69], the cooperative driving at blind crossings is also studied.


**Fig.1.10** Cooperative collision avoidance system.

A safety driving concept is developed to denote the vehicle's free movements without collision at crossings. Later, a leaderless model is developed which is based on the pattern

communication among interacting agents such as unidirectional, bidirectional and time dependent.

### 1.6.3 Infotainment

The service under infotainment includes internet access, content sharing among vehicles, video sharing etc. The communication created among vehicle to internet is considered as a challenging task.

In [70], the author proposed a QoS framework to allow forwarding of data in the internet passing through a gateway free area in a highway scenario. This involved a proxy based vehicle to internet protocol along with prediction based routing algorithm and IEEE 802.11p scheme.

Video sharing over VANET is also another infotainment service that attracts more attention. In [71], the author proposed a quality driven model for delivering the video packets in urban VANET coherently. This is based on routing and mobility management on the basis of Mobile Internet Protocol Version 6 (IPv6). Meanwhile, another author developed an adaptive video streaming model for providing video streaming services in the highway.

On the basis of cooperative relay that happens between vehicles, a video data can be downloaded by the vehicle using either multi-hop link or direct link to the Road Side Unit (RSU). This approach uses a suitable number of video enhancement layers in order to improve the quality of video.

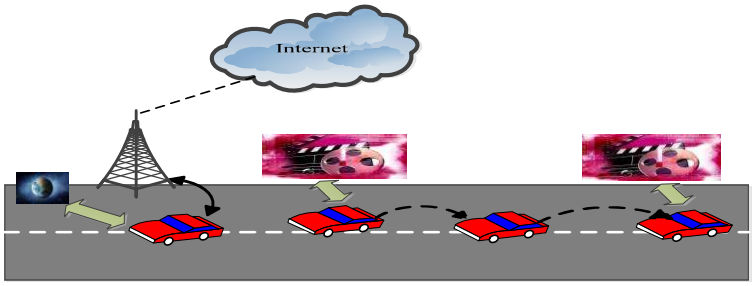



**Fig.1.11** A scenario of video services.

A robust scheme on Streaming Over Vehicular (SVC) over an urban VANET was proposed by Razzaq et al. with network coding and path diversity [72]. This robust scheme determined the quality of all candidate paths using gray relational analysis. Later, assigned paths to various layers based on their significance.

The nodes that lie along the transmission line may maintain a record of the packets received and keep at buffers as the backup of lost packets. A mechanism known as Cooperative Video Streaming over Vehicular Networks (CVS-VN) was proposed by Lee et al. [73]. This mechanism used a new video codec known as Co-SVC-MDC that split the multimedia stream into various descriptions. The requester can be achieved the QoS in case of multimedia display through the 3 to 3.5G network channel of the requester. In [74], the author proposed an approach based on video for network code selection as well as packet scheduling. This considers the importance of network state, deadlines of video packets and packets transfer to neighbor nodes.

Some of the applications of IoV are listed as follows.

- **Traffic Congestion Control**

  IoV [75] has brought a drastic change in traffic control management, mainly in urban areas, by providing the ability to predict traffic conditions, road conditions, etc.

- **Road Accident**

  With the help of IoV, the information related to the crash car can be automatically sent to the emergency teams. So, it plays a vital role in saving lives.

- **Safety Drive**

  Collision of the vehicles can be avoided by using sensors to predict collision and to alert the drivers beforehand. Status and emergency messages are provided to the drivers with the help of IoV applications. Emergency messages will arise in certain conditions such as accidents, traffic jams, and poor condition of the road.

- **Entertainment**

  Vehicles connected to the network are provided with online streaming videos, music, and information.

- **Easy and Comfortable Services**

  Enabling of accessing a car remotely provides various services such as tracking of the lost vehicle, unlocking of the vehicle door, and various other activities. All the necessary information related to transportation can be provided for all the vehicles connected to the network. The necessary information can be traffic data, parking data, etc.

## 1.7 Challenges in IoV

The main purpose of IoV is that it allows the integration of multiple devices, things, vehicles, users in the networks to provide the best communication capability which is operational, manageable, credible and controllable.

This results to a complex system. However, IoV have different applicability in comparison to other networks. At the same time, it also needs special requirements. Therefore, by considering both the aspects various challenging issues on [76], the research and development of IoV have evolved.

Some challenging issues exist for adjusting all the vehicles over heterogeneous networks in order to introduced sustainable services in real time. This is because; there is a limitation in network bandwidth, lower service platforms, mixed wireless access, and complex environment.

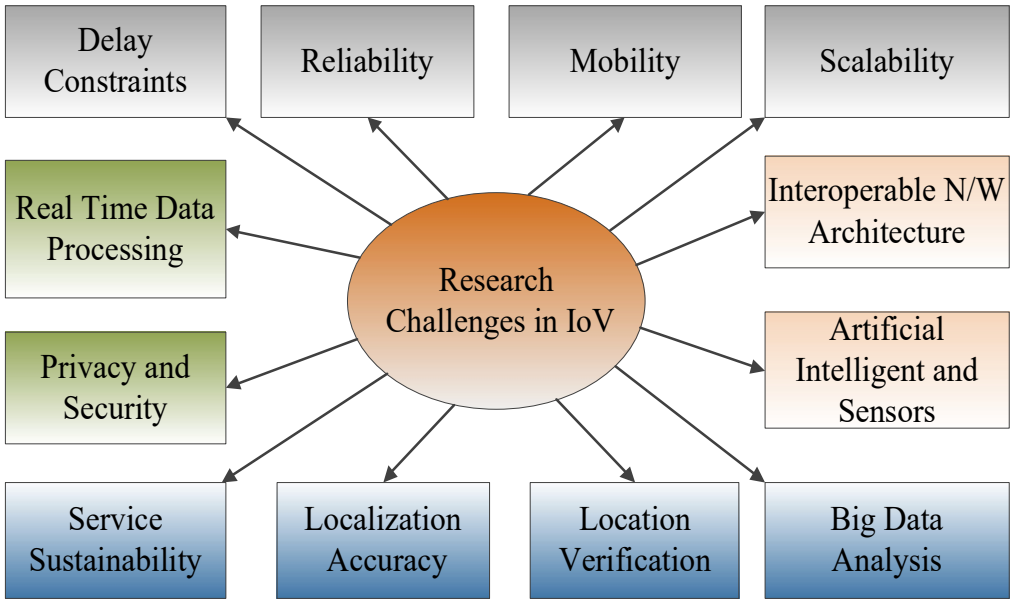



**Fig.1.12** Research challenges in IoV.

### 1.7.1 Hard Delay Constraints

Several applications of IoV have hard delay constraints. Even though, they may not use high bandwidth or data rate. In an automatic highway system, if brake is applied the message is transferred within a certain time in order to avoid car crash. In such type of application, a minimal delay might be crucial instead of average delay.

### 1.7.2 Requirements of High Reliability

Applications based on driving and transportation is usually sensitive to safety. Therefore, the requirement for such an application is high reliability. But, due to several factors such as poor network stability, large network scale, complex network structure, high reliability in IoV is difficult to achieve. Hence, special design needs to be conducted in several layers starting from networking protocols to applications. The devices such as sensors, vehicles and the hardware used for communication purpose can develop a fault which may lead to

incorrect communication, incorrect information, etc. Therefore, IoV is very important for safety purposes (reliability).

### 1.7.3 Requirement of High Scalability

This is also another challenging issue in IoV. As IoV consists of very large number of devices or node or in terms of deployment territory. Therefore, this large scale requires high scalability in IoV technology.

### 1.7.4 Privacy and Security

In IoV, keeping equal weightage between privacy and security is one of the challenging issues. The delivering of trustworthy information from the source to destination is important for the receiver. But, the trustworthy information can go against the privacy required by the sender.

- **Data Security**

  In IoV environment, data security is needed as it integrates various technologies. It is also a target for cyber-attacks, which leads to the leakage of information, as it is an open public network.

- **Location Privacy**

  Vehicular communication depends on the periodic beacon information obtained from the network. This is due to the high mobility in the adhoc network environment. The parameter such as location, direction, velocity, acceleration, vehicle types etc. are included in periodic beacon information [77].

  To reveal the location of a vehicle is a huge privacy concern. Therefore, the vehicles will utilize the location of a vehicle for communication purpose without exposing the location information. This leads to considering location privacy as a challenging task [78]. Even though there are techniques such as mix zone [79], silent period [80]

and pseudonym switching [81] have provided suggestion on privacy concern but, the concern is still unresolved. The main issues regarding privacy concern are as follow:

- Mix zone is workable on larger zone area with multi-lane roads. But this is not suitable on single way roads.
- Silent period is useful only on non-real time ITS applications. But not suitable on real time applications.
- Pseudonym switching is suitable in case of large vehicle density. But not suitable in case of environment with lower density of the vehicle.

### 1.7.5 Service Sustainability

To assure the service sustainability provided by IoV is also another challenging issue. This requires high intelligence approach and user-friendly network design.

### 1.7.6 Localization Accuracy

The accurate localization of the vehicles is important and consider as a challenging issue because of the accuracy needed in vehicular communication environments. The accuracy needed in such case is quite higher as compare to the accuracy provided by the localization based on GPS [82]. There are three issues are needed to address for fulfilling the accuracy requirement:

- Localization based on GPS contributes accuracy of 5m while Vehicular communication environments required accuracy of 50cm [83].
- Localization based on GPS does not consider speed of the objects while in vehicular communication environment speed is considered as the important constraints [84].
- Degradation or even unavailability in the quality of GPS signals in crowded urban environments [85].

### 1.7.7 Location Verification

In vehicular communication, the location verification of the nearby vehicle is considered as a challenging task. The main reason is due to the trust worthy issues in vehicular communication. There are several techniques suggested for location verification purpose such as cooperative approach [86], beaconing based belief [87], directional antenna [88] etc. Further some of the issues need to be addressed in location verification technique and it is defined as follows:

- The untrusted neighbor in cooperative verification.
- The overloading in beacon technique.
- The infrastructural cost in directional antenna technique.
- The limitations that occur in range based technique of vehicular communication environment.

### 1.7.8 Big Data Analysis

The information collected from a huge number of devices is extremely large. So, storing and processing of these data is one of an important challenge in IoV. In the case of vehicles without drivers, i.e., automatic vehicles will process around 1GB of data every second. To stored and analyze all this information, big data analytics and cloud computing are used.

### 1.7.9 Mobility

It is a challenging task to keep a record of the vehicles moving at high speed. Because the network topology frequently changes due to the variation in the speed of the vehicles, and it is complicated to keep the actors in the network connected to transmit the resources.

### 1.7.10 Interoperable Network Architectures

There is an extraordinary requirement for upgraded protocols and algorithms for communications which may have the option to encourage and to deal with the mobility in

the domain of Internet of Vehicles. Until now, it can be noticed that there is difficulty in making an efficient and interoperable execution, which may fulfill all the IoV limitations and prerequisites required for the IoV.

### 1.7.11 Artificial Intelligence and Sensors

Interaction of vehicles is done based on the specific measure of the sensor's information. This information sensed through different sensors should be combined together before utilizing in settling on vehicle choice. For solving real world problem Artificial Intelligent (AI) simulate the intelligence of human into a machine to make the intelligent machine. Data Engineering (DE), Natural Language Processing (NLP), Expert System (ES), Intelligent Data Mining (IDM), Fuzzy System (FS), Meta-heuristic algorithms (MHA) and Knowledge Discovery (KD) is incorporated into AI. Nowadays, artificial intelligence technology is used in IoV but needs a test on real situations before vehicle travelers can confidently utilize full self-driving.

### 1.7.12 Real-Time Data Processing

There are situations where parallel data processing only is not enough. So, in that case, a combination of sequential and parallel data processing is required. In IoV, parallel data collection, processing, and analysis of big data are very much essential.

## 1.8 Security in IoV

In IoV environment, different types of technologies need to be integrated to make it secure [89]. The requirement of data security is increased due to the substantial number of vehicles [90]. IoV is vulnerable to security like other technologies, as introduced by Zhang [91-92], and it has become more vulnerable to cyber-crimes. In vehicle-infrastructure communication, vehicles were operated in unprotected environments that have serious security problems. Several cybercriminal activities can exploit the vehicular data and can operate on the vehicles automatically [90]. They can turn off the vehicles, unlock the doors

and break etc. Conferences held regarding cyber security, some authors have demonstrated on attackers controlling the activities of the devices using some software [93]. This demonstration shows the dangers of security problems in IoV.

**Table 1.1** Security requirements for IoV.

| | |
|---|---|
| Data Authentication | The identity of the device needs to be verified before the transmission of the data. |
| Anti-jamming | It is a mechanism to avoid any malicious devices to interfere in the communication process among the devices. |
| Access Control | Vehicles should be allowed to access only the services provided by the IoV. |
| Availability | The communication between different vehicles needs to be guaranteed. |
| Data Non-repudiation | It is a process to guarantee that a vehicle can't preclude the authenticity of the other vehicle. |
| Availability | To ensure the communication between the vehicle in different conditions. |
| Data Integrity | It is the process to ensure the data delivered is correct or not. |
| Confidentiality | Data transmission among the vehicle must be carried out in a secure manner. So that attackers cannot utilize the data. |

Some other authors [94] also explained the complexity of attackers controlling vehicle communication through sensors and controlling the vehicle's commands. So, security concerned is needed to be solved from the severe consequences faced by passengers, drivers, and vehicles. Therefore, security on IoV is given a high priority, and some institute has come forward to solve the security issues. The National Institute of Standards and Technology (NIST) incorporated the security infrastructure to IoV technologies [95-96] and many other authors also proposed a secure communication platform.

## 1.9 Motivation

Due to the rapid evolving of communication and computation technologies, recently huge commercial and research interest has been shown on IoV. Therefore, it attracts several researchers and companies. IoV focuses mainly on the intelligent integration of vehicles, human, things in the environments. This is larger networks that have the ability to provide services on larger cities including whole country. Additionally, IoV have the capability to acquire, manage and compute the dynamic and large-scale data for vehicles, human, things existing in the environment in order to improve the sustainability, extensibility, computability of the complex network and information system. It has also been estimated that 25 billion things are likely to connect to the internet in the near future. Hence, developing IoV technology is necessary.

Considering the significant information of IoV, this motivates the researchers to designed and developed IoV. The designing and development of IoV is classified into three categories. In first category, commercialization of VANETs related issues is noted. Secondly, the increased in traffic casualties are examined. Lastly, the opportunity lying ahead of IoV is examined.

### 1.9.1 Commercialization of VANETs

Considering the potential of VANETs in terms of safety and efficiency of traffic with less operational cost, this cannot attract the attention of commercial industries for the past decades [97]. The reasons behind the lack of commercial interest in VANETs are as follows:

Firstly, it focuses on the framework of VANETs. The framework does not guarantee global applications and sustainable services by ITS. The reason is because of pure adhoc network architecture. In case of vehicles that are being on road get disconnected from the adhoc network, the services provided by the network get loses. This is because; the vehicle is not able to connect with other alternative networks [98].

Further, the internet connectivity cannot be guaranteed in the present framework of VANETs. Hence, commercial applications are not made available to passengers and drivers. This is because of the commercial applications depending on reliable internet connectivity [99]. Even though in our daily life there is huge growth of personal devices, these devices cannot be communicated in VANETs. This is because of incompatibility in the network architecture [100]. In current VANETs architecture, intelligent decisions in terms of big data mining driven computations are not possible. The main reason is the storage and computing constraints and non-availability of cloud computing services [101].

The accuracy provided by the ITS applications services is significantly lower even after considering the risk of the services regarding better driving experiences. This is because of the computation of VANETs traffic environments using the local knowledge. In vehicular network, operations depend highly on the cooperation among the network users. Due to the dependency, the reliability of the VANETs services diminished [102].

### 1.9.2 The Increasing Traffic Casualties

In case of traffic casualties, the three major issues involved are pollution, safety and efficiency. These issues are major causes of concern for designing and developing the IoV architecture. Therefore, the IoV architecture would provide a vehicular communications framework with more reliability in comparison to VANETs for advanced ITS applications. This reliable framework for vehicular communications leads to reduction of traffic casualties [103]. Various surveys have reported the increasing traffic casualties all over the world. Some facts regarding the traffic casualties are describe below.

Based on the World Health Organization (WHO) report, the estimated worldwide deaths due to various traffic accidents that happen on road is 1.25 million per year [104]. The total deaths per day are estimated as 32876 approximately. The young person in the age range from 15 to 29 has suffered from highest road traffic injuries in the last decades and this has

been the major reason of casualties. Meanwhile, on the basis of some other report road crashes has a result to huge economic lost [105].

The other reason behind traffic casualties is the huge increased in the number of vehicles on road. The increased in vehicles causes air pollution in the capital cities. Therefore, a reliable vehicular communication is needed urgently in order to reduce casualties cause by traffic on road and for safety purpose.

### 1.9.3 Market Opportunities

IoV has provided huge market opportunity to various sectors such as automobile industry, software industry, IT equipment manufacturing industry, and Internet service providers. Across the world, significant increase of the number of vehicles on road has been predicted [106]. In the coming years, the increased in the motorization rate would lead to congestion of road there by resulting to longer travel time. For every 5 minutes wasted in travelling can generate Euro 25 billion revenue for every year by next decades [107]. Another key objective of IoV is the utilization of travel time effectively.

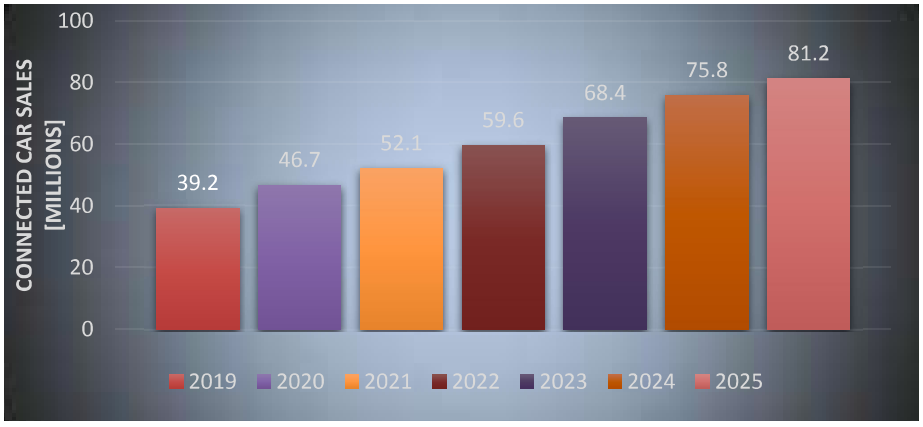



**Fig.1.13** The prediction of car sales with some form of connectivity till 2025.

The main key in the designing and developing of IoV architecture is the current advancements and increased in the market penetration rate of IoT [108]. With the growth of IoT, among all the industries automobile industries became one of the fastest growing

industries [109]. According to Figure 1.13, it has been estimated that by 2025 almost 80% sale of the new cars would be connected to some advanced drive technology. Hence, the predicted increased in the economic value by 2025 from IoV technology is in the range from $210 to $740 billion [110].

After considering all the advantages of IoV technology in the real time environment including the safety, security as well as the increased in the economic value motivates to work in the modeling of Internet of Vehicle keeping the welfare of the people as the most significant point.

## 1.10 Problem Definition

Recently, IoT has brought various changes in the existing research field by including new areas such as smart transportation, smart home facilities, smart healthcare, etc. In smart transportation systems, vehicles contain different components to access information related to passengers, drivers, vehicle speed, and many more. This information can be accessed by connecting vehicles with Internet of Things leading to new fields of research known as IoV. IoV is an integrated and open network system that consists of multiple components such as vehicles, users, things and networks. IoV has turned into a most encouraging and fastest developing research area. The setup of IoV consists of many sensors to establish a connection with several other sensors belonging to different environments by exploiting different technologies. The communication of the sensors faces a lot of challenging issues. Some of the critical challenges are to maintain security in information exchanges among the vehicles, inequality in sensors, quality of internet connection, and storage capacity. Besides, employing several vehicles, several vehicles moving on the road as an eye witness to capture the information about the incidents happening on the road is also another challenging task. Meanwhile, with the advancement of vehicle's traffic information processing and communication capability in the 5G and beyond IoV (5G&B IoV) network widely used for the vehicle-to-infrastructure transportation communication. Firstly, the protection of the user's (vehicles) privacy at the time of information sharing and secondly, users lack the

motivation to share the traffic information with RSUs are two major concerns in the 5G&B IoV networks.

Additionally, privacy is the most important part of VANETs since various attacks such as location tracking and identity revealing steal sensitive information to create considerable risk for human lives. The attacker changes confidential information such as speed, direction, path, location of vehicle owner, and exploits its privacy. The existing privacy-preserving schemes like pseudonym schemes, anonymous signing protocol, group signature, and authentication-based schemes, mix zone and silent period, etc. are inefficient in terms of storage, privacy-preserving, and implementation. Furthermore, they impose high overhead and converges very slowly.

Lastly, Vehicular communication has attracted reasonable attention recently from both manufacturers and the academic world. This is due to the high demand for on-road safety by road users. Thus, many approaches have been considered for vehicle communication in order to augment the existing on-road safety. One of these approaches is multipath transmission, which supports path diversity and minimizes delay and load balancing, which in turn improves data packet delivery. In multipath video streaming transmission, the selection of the best vehicle for video packet forwarding considering the junction area is a challenging task due to the several diversions in the junction area.

## 1.11 Research Objectives

Some of the main objectives are as follows:

- To designing a new IoV framework consisting of seven-layered architecture, including the security layered, which provides seamless integration by communicating the devices present in the IoV environment.
- To develop a novel Adaptive Neuro-Fuzzy based Payment using Blockchain (ANFPB) transportation communication scheme that allows users to anonymously share the traffic information with RSU in the 5G&B IoV network.

- To design an IoV model that encourages the user participation on the road.
- To propose privacy assures rewarding system to reward the active participating vehicle based on the contribution to the services.
- To design privacy preservation, authentication system to secure the passenger's privacy this is cryptosystem and pseudonym.
- To develop a Junction-Aware vehicle selection for Multipath Video Streaming (JA-MVS) scheme.

## 1.12 Accomplishment and Contribution

The following paragraph illustrates the research works that have been done towards achieving the objectives as a contribution in the field of Modeling of Internet of Vehicle.

To overcome the challenging issues, we have designed a new framework consisting of seven-layered architecture, including the security layer, which provides seamless integration by communicating with the devices present in the IoV environment. Further, a network model consisting of four components such as Cloud, Fog, Connection, and Clients has been designed. Finally, the protocol stack which describes the protocol used in each layer of the proposed seven-layered IoV architecture has been shown. In this proposed architecture, the representation and the functionalities of each layer and types of security have been defined. Case studies of this seven-layer IoV architecture have also been performed to illustrate the operation of each layer in real-time. The details of the network model including all the elements inside each component have also been shown. This proposed architecture provides a secure IoV environment and provides life safety. Hence, safety and security will help to reduce the cybercrimes occurring in the network and thereby provide good coordination and communication of the vehicles in the network.

We propose a JA-MVS in a vehicular network. The JA-MVS scheme transmits video packets considering the different positions of the on-road junctions and the Signal to Interference Plus Noise Ratio (SINR) as the signal quality for best forwarding vehicle

selection. In the junction-aware algorithm, a vehicle that is ahead of the junction and moving toward the Destination Vehicle Node (DVN) is given higher priority to establish reliable video packet forwarding in the junction area. The SINR is an important metric for evaluating vehicle signal strength considering the urban scenario, which has a lot of obstacles that affect vehicle signal during transmission. The simulation results validate that the JA-MVS scheme significantly improves the video transmission performance in relation to the increase in quality of the video streaming, with a lower Packet Loss Ratio (PLR) and higher Structural Similarity Index (SSIM) and a decrease in the overall End-to-End Delay (E2ED) of the video packet transmission. In addition, the simulation shows that the overall performance of the JA-MVS outperformed the two baseline schemes of Junction-Based Multipath Source Routing (JMSR) and Adaptive Multipath geographic routing for Video Transmission (AMVT).

We proposed a Novel Adaptive Neuro-fuzzy based Payment using blockchain scheme to preserve the privacy of vehicles in the process of information sharing and also encourage vehicles to participate in the information sharing with RSU in IoV network. A smart contract is also proposed to register the vehicles themselves using an identity exchange process to provide more secure privacy from any attackers to access the contents in midway. Meanwhile, we also introduced the rewarding of most active users in the IoV network to encourage the users to participate using the neuro-fuzzy technique algorithm ANFPB.

We propose the framework of network model has been designed in such a way to maintain its functionality, privacy, security and provides rewards to the witness. Later, we also assume that the incidents occurring on the road have been captured by an already existing mechanism. Meanwhile, we assume that users have multiple pseudonyms. These pseudonyms are exchange periodically among the users to ensure anonymous communication so that the attackers or outsiders cannot track easily. Further, we extend the cloud computing technology by implementing a new layer known as Fog layer. Fog layer is mainly used for storing instant images or data, whereas cloud layer is used for storing large amount of data. Lastly, to encourage the user participation on the road, we proposed privacy

assure rewarding system for making the vehicle to reward based on the contribution to the services.

We suggested a novel LAP for VANETs in which TA chooses a shared secret key $k$ between $R_j$ and TA, it is stored in the database of TA. We proposed an informal security analysis for authentication, in which we demonstrated that our suggested system meets all VANET security standards. The proposed method not only integrated authentication, but also keeps the vehicles secret. Furthermore, we simulated and then compared our schemes to other relevant schemes to determine its efficiency and performance. Its provide better performance as compare to the others schemes also comparing our protocol to other relevant protocols reveals that it is more suited to real world environments.

## 1.13 Organization of the Thesis

The thesis is organized as follows: In the first chapter, the introduction of Internet of Vehicle is given along with the applications and challenging issues of Internet of Vehicle. The second chapter describes the literature review of the techniques related to modeling of internet of vehicles. The drawbacks of the existing techniques are also mentioned in the chapter. The third chapter includes the proposed model on video streaming in urban vehicular environments. In the fourth chapter, an efficient light weight authentication scheme has been propose. In the fifth chapter, a proposed model on Adaptive Neuro-fuzzy based payment scheme using blockchain to ensure privacy of vehicles in 5G and Beyond (5G&B) networks is describe. At last, the sixth chapter represents the conclusion of the thesis by summarizing all the research work carried out on modeling of internet of vehicle.

# Chapter 2

## Literature Survey

Recently, IoV evolved as new smart transportation technology based over IoT that provide an intelligent interface through ubiquitous sensing capabilities. This smart transportation system known as IoV consists of various vehicles connecting over wireless network through smart sensors, where information are collected and shared/uploaded to the nearby road side unit. The information is related to the vehicle locations, passengers, drivers, vehicle speed, road traffic condition, and many more. To access these information vehicles contains smart sensors or mounted camera to take pictures and internet connectivity. The setup of the IoV consists of many sensors to establish a connection with several other sensors belonging to different environments by exploiting different technologies. The communication of the sensors faces a lot of challenging issues. Some of the critical challenges are intermittent services, requirement of higher bandwidth, maintaining security in information exchanges among the vehicles, inequality in sensors, quality of internet connection such as communication channel interference, and storage capacity.

In this chapter to overcome the critical challenges, we review the foremost research work in the field modeling of IoV. In the paper [111], a new framework was proposed consists of six-layered architecture, including the security layer; which provides seamless integration among heterogeneous vehicles. Further, a network model consisting of four components such as Cloud, Connection with different Clients to ensure compatibility has been designed for IoV. Furthermore, data analytics layer was designed to ensure storage and remove the redundancy of high data volume. Finally, security layer also designed to ensure security such as intruder detection or network tapping.

Researchers have developed various communication layered architecture [112-114] to overcome the current issues and challenges of the IoV network. In the paper [112], authors have claims that proposed model is human-attraction architecture and cover the high-speed

vehicle mobility, security with proper allocation of resource and useful for delay tolerant network. In continuation to solve these problems, researchers in the paper [113] predict the traffic congestion using cloud based mobile communication and provide real time dynamic route to alleviate congestion.

Whereas in the paper [114], authors proposed Software Defined Network (SDN) architecture to instantly start the services as per as requirement of IoV network using capabilities of cloud network. However, these models are restricted to only one side of the network and cannot able to solve the challenges of data communication, security and their storage and management fully.

In addition, human- attraction architecture [112] was confined to only small number of vehicles and cannot handle to big data analytics; dynamic route [113] prediction is unrealistic in nature because of complex implementation. Therefore, there is need to develop more concise and relevant architecture having proper component in details, which must solves the pure IoV network challenges. In Table 2.1 below some of the existing IoV architecture models, their different types of layers, and their functionality have been noted down.

The modeling and implementation of IoV architecture is motivated by the contemporary IoT communication technologies related to Dedicated Short Range Communication (DSRC), Long-Term Evolution (LTE), Cloud Computing (CC), Worldwide Interoperability for Microwave Access (Wi-MAX). Using these recent technologies in smart transportation system, IoV reveals several issues related to diverse inter-connected devices, data protection issues, bandwidth and channel allocation, data integrity etc. To overcome these prominent issues Layered Based IoV Architecture is one of the most feasible functionalities and modeling to achieve the heterogeneous IoV network requirements. In this chapter, we'll go over some of the most popular IoV modeling strategies for maximizing network performance. Finally, future research and development directions in the domain are identified based on open research concerns and challenges in the IoV environment.

**Table 2.1** Exiting layer based IoV architecture.

| | | |
|---|---|---|
| A survey on the security issues occurring in VANETs [115]. | They illuminated the necessities of security, its significance, attacks occurring at various layers, and different techniques adopted to handle the several attacks. | Shows the signify-chance of security on different layers. |
| A review on attacks detection mechanisms carried out on intelligent systems for transportation using VANETs and IoV [116]. | A survey has been performed on the attacks along with the possible effects and their working principals. Further, a survey was introducing of solution utilizing various detection mechanisms discussed in the literature survey. Lastly, based on the methods used, detection architecture, infrastructure, and various mechanisms, a survey was also presented. | This paper includes attack detection along with possible solutions. |
| Security and attack analysis for vehicular ad hoc network—a survey [117] | Details discussion about the security architectures along with well-known protocols and standards for security is carried out in this paper. Several threats to VANETs that are discussed here are crucial, which leads to difficulties in VANET implementation to make it reliable to the real world. | Study about reliable VANET on the basis of security and attack taking place on VANET. |
| A comprehensive survey on security services in vehicular[118] | In this paper, review on VANET system model, VANETs characteristics, security issues occurring in VANETs, security services taking place in VANETs is performed. Further, a brief discussion on security attacks along with possible defence is also included. | It includes security issues occurring in VANET services. |
| Survey on security issues in vehicular ad hoc networks [119] | This paper performed a survey on attacks by introducing attack classification. Further, the countermeasures on attacks are also discussed. | This covers the classification of attacks along with defences. |

## 2.1 Layered Based IoV Architecture

This section will briefly discuss about the various layers based IoV architecture with their advantage and limitations. Different types of IoV architecture based on the interaction of various innovations in the IoV environment have been identified by the researchers. In the paper [120, 14], the author develops three-layered architecture.

First layered consists of sensors deployed in the vehicles to collect the data from the environment and record certain information such as vehicle location, patterns of driving, etc. Follow by the second layer, known as the communication layer. This layer supports various wireless communication approaches, including vehicle-sensor, vehicle-vehicle, vehicle-infrastructure, and vehicle-pedestrian. The third layer incorporates statistics tools, storage support, and infrastructure that consist of intelligent IoV.

In the paper [121] also, the authors have designed a three-layered architecture such as client layer, connection layer and cloud layer. All the sensors that are present inside and outside of the vehicle in the client layer are responsible for capturing the information related to certain events that happen in the vehicle. This sensor senses the vehicle speed, condition of the road, air quality, collision prediction, temperature and humidity level, etc. The connection layer guarantees interoperability with all the accessible networks supporting various types of communication models. All the captured information is sent to the cloud layer providing computational power to full-fill the vehicle's requirements.

Bonomi [19] developed a four-layered architecture of IoV. The first layer is responsible for vehicle’s software for V2V communication. The next layer is responsible for connection among all the devices in the IoV where vehicles are located at any given time. The operation layer ensures compatibility with various application schemes to circulate the flow of information management. The last layer is the cloud layer, which defines the various types of cloud possible for accepting on-demand services.

Wan et al. [122] designed a three-layered IoV architecture. One of the layers is a vehicular layer that manages the internal sensors of the vehicles and captures the information through wireless technology that lies within a short-range. This architecture is mainly designed for exchanging information in a short-range. To exchange the information in longer range, multi-hop communication is needed. The cloud layer is responsible for historical information related to traffic and load balancing of multiple cloud services.

Kaiwartya et al. proposed five-layered IoV architecture such as 'perception', 'coordination', 'artificial intelligence', 'application', and 'business' [22]. Perception layer precepts the information through sensors and actuators, which are deployed in the vehicles and gather the data from the different components of the vehicle. The data may be related to traffic conditions and associated gadgets such as tablets, smart watches, headphones, etc. Coordination layer coordinates the module present in a communication network to perform secure information transfer. This information is processed in the cloud layer, which is responsible for storage, processes and analysis of the information obtains from other layers and provides the best option to select the applications for intelligent services, traffic safety, multimedia, etc. The business layer is mainly related to developing a business model by applying statistical analysis.

The authors in [123] proposed IoV architecture consisting of three-layered mainly for D2D communication purposed. The connection between the devices in the network is presented in the first layer. The devices are either connected directly to one another or they are connected through the gateways present in the network to carry out different types of communication such as wired and wireless. The next layer is for roaming and IP connection, which is responsible for heterogeneous vehicle connectivity and provide gateway to share information seamlessly. The last layer is for application purposed like smart homes, smart gadgets includes watches, keys, voice over command to start/stop engines of air conditions of vehicles. Those applications provide better management to users which enable them to control their vehicles from distant.

In this regard, different type of prominent work related to IoV architecture models, their different types of communication layers, and their security level are listed below in the Table 2.2.

**Table 2.2** IoV architecture with their IoT communication.

| **Types of IoV architectures** | **Different Layers** | **IoT Communication models** | **Security level** |
|---|---|---|---|
| Nanjie et. al. | Three layers: Client, Connection and Cloud | V2V,V&R,V&P,V&I | Security as a service |
| Wan et. al. | Three layers: Location, Cloud and Vehicle | V&R, V2V | Cross-Layer |
| Gandotra et. al. | Three layers: Network management, D2D area networks and D2D application | Non-critical applications (D2D-N). Backhaul applications(D2D-B), Direct D2D (D2D-D), Critical application (D2D-C) and Direct M2M (M2M-D) | Not Specified |
| Matthew et. al. | Three-layer: Perception layer, Network layer, Application layer | V2V,V2R,V2H,V2S, | Not Specified |
| Bonomi et. al. | Four Layers: Endpoints layer, Infrastructure layer, Operation layer, Service layer. | V2V, V&R, V&I | Cross-Layer |
| Kaiwartya et. al. | Five Layer: Perception, Coordination, AI, Application and Business | V2I, V&R, V2V, V&P, V2S, | Security Plane |

**Limitations:**

- Above proposed models do not clearly define the protocols used in each layer. Instead of using appropriate number of layers, less number of layers are proposed in the models with more complexity, it is better to use more layers noting each protocol used in each layer and their functionality in detail description. The complexity will also reduce when the numbers of layers increased with simplified description. This will make the architecture more simplified and ensures secure interconnectivity among the devices considering various technologies.
- Existing IoV architecture does not have security layers to perform authentication, authorization, etc. to make a secure environment. No layer has been provided to performed integration of communication intelligence such as selecting the best network to transmit information or accessed service. These architectures have a limitation in the interaction of passengers and the drivers by giving just notification through the devices connected in the network.
- The information has been transmitted without any proper pre-processing, and this causes congestions in the network by increasing the number of vehicles. In order to solve these drawbacks, we have designed a model of IoV architecture consisting of seven-layered which provides more transparent interconnectivity among the components or devices present in the IoV network that diffuses the data. Within this seven-layer, one of the layers is a security layer that provides authentication, authorization of all the information or data transmitted among the various entities in the IoV networks.

## 2.2 Junction-Aware Multipath Approach

In this section, video data transmission considering the characteristics of IoV and video streaming applications are discussed. Current multimedia applications require high capacity communication links to facilitate high speed data transfer rate. Video applications require

stringent video quality requirements including minimum delay, minimum packet drop, and efficient bandwidth utilization [124-125].

### 2.2.1 Street-Oriented Vehicle Selection

The normal street-oriented video data forwarding in vehicular communication is discussed considering the different existing works that do not consider the junction area during video forwarding. For example, in Yaqub, et al. [126], a Collaborative video Retrieval (CoRe) scheme has been proposed in order to address the issue of a bandwidth-constrained cellular network, which affects the quality of a video transmitted by a vehicle. The CoRe scheme enables vehicles to transfer quality video from the Internet and distribute it among other vehicles; that is, neighbor vehicles that reside in a normal street during data forwarding. The collaborating vehicles are selected by taking advantage of their on-road characteristics. These on-road characteristics include their obtainable cellular bandwidth, relative velocity, connection period and Euclidean distance. In addition, the neighbor vehicles, which are the collaborating vehicles, download the video stream via the cellular link and disseminate it to a requesting vehicle based on the DSRC protocol. However, only on-road characteristics have been considered; the junction's characteristics have not been explored. Further, a Multiple Unicast Path-Forwarding (MUPF) scheme has been proposed to tackle the challenges of the traditional IP-based communication in the vehicular network. The scheme explored Information-Centric Networking (ICN) and numerous unicast forwarding paths for data packet forwarding. In addition, the selection of the routing paths considers the issue of link breakage and link quality in relation to the mean response time. However, the situation in which the forwarding vehicle is in the junction area has not been explored.

A cooperating neighbor vehicle solution based on the Game-Theory approach for Platoon-centric (GT4P) driving has been suggested to address the challenges of the short contact time among vehicles during multimedia data transmission, which could lead to delay and video packet error [127]. Thus, the video packet error decreases the Quality of Experience (QoE) of the disseminated video. Therefore, a set of neighbor

vehicles, which are navigating in the same direction and are willing to collaborate, forms a platoon member that serves as a forwarding vehicle. The GT4P approach improves collaboration among neighbor vehicles by giving a reward to participating vehicles in the platoon. The collaborating platoon members are formed by considering link quality, travel path and mobility parameters including direction, distance, and speed, which minimizes the effect of vehicle mobility on the video streaming transmission. However, the platoon members at different points in the junction area are not considered. Thus, there is a need to explore the junction characteristics.

Similarly, a comparative analysis for platoon-centric video streaming transmission in autonomous VANETs has been suggested to assess and ascertain the QoE for shared video flows [128]. Different vehicle distances between the source and destination vehicle and various video characteristics are employed. Thus, the effectiveness of the platoon-centric video transmission is justified considering different video metrics. Further, platoon-centric driving offers a collaborative navigation arrangement for a set of vehicles with the same navigation route such that the member vehicles in the platoon keep almost a fixed distance among themselves. In a typical platoon approach, the cruise control system utilizes the on-board sensors for example, laser or radar to estimate the distance between vehicles and then adjust their speed. Further, a member vehicle obtains information from the platoon leader via vehicle-to-vehicle communication. Thus, collision is minimized through communication with vehicles ahead. The platoon approach alleviates the effect of the short contact time that leads to video packet loss or error in the time of video transmission. However, the whole approach does not look into junction-area-based video packet forwarding.

In order to address the issue of high latency in locating a possible content provider in an information-centric network, a Preference-aware Fast Interest Forwarding (PaFF) method for video streaming has been suggested [129]. In the PaFF approach, each vehicle forms a Highly Preferred Content Table (HPCT) in order to preserve the content catching status of vehicles that have similar video play back behavior's and mobility parameters. Considering the HPCT, a vehicle forwarder that employs a preference mechanism is explored to choose

the next hop of relevant video packets to minimize delay and improve reliability. The selection of a potential forwarder vehicle for the content delivery depends on fundamental mechanisms including the estimation of similar mobility parameters of neighbor vehicles, preference agreement and potential vehicle discovery beyond one-hop neighbor vehicles. However, in the mobility parameters for potential forwarding vehicles, the various points at the junction have not been considered. Therefore, the next subsection discusses video transmission considering the junction areas of roads.

### 2.2.2 Junction-Oriented Vehicle Selection

In this subsection, the existing solutions that consider road junctions during video data forwarding are discussed. In the multipath setup, very few research studies have considered the realistic nature of VANET roads; for example, in [130-131]. The intersections and junctions of roads need to be considered to select vehicles for multipath transmission. The incorporation of junctions/intersection into multipath transmission offers more realistic and efficient and higher- quality video streaming. Thus, in Sermpezis, et al. [130], an analytical Junction-Centric Multipath Source Routing (JMSR) mechanism has been suggested. JMSR features include junction-aware logics, the multipath route from the source to destination and the source routing scheme. The JMSR employs geographic routing protocols, meaning that the locations of the junctions of a street are leveraged through the street's digital maps for data forwarding purposes. In the multipath setup, two paths are preserved concurrently considering the numerous junctions which a routed data packet has to traverse before reaching its destination. In addition, the JMSR embeds routing details into an individual packet, based on the source routing standard. The source routing standard is set-up in such a way that every individual vehicle in the path knows the route the packet must traverse. However, in JMSR, all vehicles are partitioned or grouped into different routes of paths, and then the cost of each path is calculated before being selected as the path for data forwarding. This approach is prone to high overhead and delay, which is a critical issue in video streaming requirements. In addition, the JMSR updates the information about the position of

other vehicles when the position of the destination vehicle changes. Since it is believed that vehicles are moving very quickly, there is a frequent change of position; thus, it is important to consider the different points of the junction area and the direction of the vehicle at the junction. The different points of the junctions that have not been considered include the vehicle after the junction, before the junction, and inside the junction. The vehicle position, road-ID and traffic status can be employed to estimate whether a vehicle has exited the junction and has taken a direction towards the destination vehicle. Thus, video packet loss can be minimized since the most optimal vehicle is considered as a forwarder at the junction area.

In Salkuyeh and Abolhassani [131], an adaptive multipath video streaming method based on geographic routing has been suggested. The adaptive scheme selects multiple paths, depending on the volume and lifetime of the video to be transmitted from the source to destination. The route connection probability has been employed to select the best route. The connection probabilities are divided into two, namely street and junction connection probability, based on the cells and line of sight of the vehicles, respectively. However, the probabilistic connectivity approach does not consider the position and direction of the vehicle for connectivity. In addition, priority is not given to a vehicle that has already exited the junction and which is in the direction of the destination vehicle. This may lead to the selection of an inappropriate next forwarding vehicle in the junction, which can cause packet loss and affect the quality of the video streaming.

De Felice et al. [132] suggested a Distributed Beaconless routing protocol for pre-recorded video Data transmission (DBD) over VANETs. It is an integrated framework that handles the QoE of video services and routing protocols. DBD further advances the performance of the IEEE 802.11p/WAVE MAC layer by resolving the spurious forwarding problem. However, an adaptive backbone mechanism is not considered for the DBD. An Opportunistic Routing solution for pre-recorded Video (ORV) streaming is proposed to handle the interference of wireless fading channels [133]. The mechanism takes into consideration the interference of vehicles from the surroundings during the relay selection

procedures. Nevertheless, the SSIM index of the video streams is not considered in measuring the quality of the video. Multiple path solutions with error correction for video streaming over VANETs (LIAITHON+) have been presented; the aim of this is to reduce collision and packet loss in high data rate networks [134]. LIAITHON+ employs a multipath approach to distribute high data rate traffic into a set of paths. However, the quality of the streaming video is not measured based on PSNR and SSIM index metrics. Al-Ani and Seitz [135] present a video stream routing QoS for the multi-rate mechanism in order to achieve congestion control and avoidance. The mechanism employs the Ant Colony Optimization (ACO) algorithm and Simple Network Management Protocol (SNMP) monitoring features. The mechanism is called QoRA; it decides on paths by considering applications that QoS needs and prevents transmission flow from entering congested nodes. Nevertheless, the mechanism is not adequately benchmarked. QoE-driven and link-quality receiver-based (QOALITE) transmission is proposed to improve the quality of video while considering a challenging VANET environment [136]. A geographical receiver-based beaconless strategy has been proposed as a solution for transmitting video streams in VANETs. However, some parameters are considered in choosing the best relay node and building up reliable backbones to deliver video messages. In addition, the dynamic adjustment of the time window needs to be considered for tackling collisions. Therefore, proper vehicle selection in the junction area is not considered in some routing schemes. Consequently, an optimal next forwarding vehicle selection scheme is required that considers the junctions and neighbor vehicle mobility information and link quality to select an optimal next forwarder for video streaming in the multipath setup.

**Limitations:**

- Authors were didn't consider the video streaming in real time on various types of streets including expressway scaffolds and twisted streets, considering their impacts on video information bundle sending to accomplish quality video web based in IoV networks.

## 2.3 Efficient Lightweight Authentication Scheme for VANETs

This section discusses the current work on Location Privacy-preserving (LP-preserving) in IOVs. Moreover, we discuss the methods with their advantage for efficient privacy-preserving.

Sampigethaya et al. [137] proposed a robust Location Privacy (LP) scheme for IOV, known as AMOEBA to enhance user LP. AMOEBA uses group navigation of vehicles to achieve LP and simulate the system in streets and freeways with two passive adversary models. AMOEBA discussed several protocols such as group join and formation protocol, group operation protocol, group leaving protocol, probe data collection and group leader rotation.

Emara et al. [138] discussed a methodology to determine the secure level of privacy-preserving by incorporating an empirical vehicle tracker in IOVs. Monte Carlo analysis is also used to investigate the impact of the proposed approach on a safety application.

S. Sharma et al. [139] projected "A collaboratively hidden location privacy scheme for IOVs" to deal with the Privacy and liability using a modification of ring signature. The modified ring signature scheme authenticated all communication messages, and rings are formed using a distributed approach. The research gap of the proposed scheme is that it is not implemented on NS-2.

Garg et al. [140] provide a "Review of different approaches for privacy scheme in IOV". Furthermore authors discussed the protocol stack for IOVs and focused on WAVE with approved frequency band 5.9 GHz. Moreover, the authors examined the attributes (Confidentiality, Authentication, Access control and Availability, Privacy, Nonrepudiation, Data integrity) of secure network. In addition, the authors discussed the attack on privacy in IOVs. The main purpose of the attack on privacy is identity revealing and location tracking. The author discusses several privacy preservation schemes such as anonymous signing protocol, group signature scheme, digital signatures, mix zone method, and random encryption periods etc. to achieve privacy in IOV.

Gerlach et al. [141] suggested a "Wireless location privacy protection in vehicular ad-hoc networks" based on vehicle density. The proposed scheme provides location privacy of vehicles by "utilizing the neighboring vehicle density as a threshold to change the pseudonyms." The suggested scheme defines some density zones and computes total delay as well as delay distribution of vehicles in a density zone. With this changed pseudonyms and vehicle delay model in some predefined density zones, location tracking becomes more complicated for attackers.

Hamdi et al. [142] suggested an "Adjusted Location Privacy Scheme for IOV Safety Applications" based on a novel silent period concept. The authors discuss the shortcomings of ordinary silent period based schemes in which an accident may happen because a vehicle stops sharing its speed, location and direction information. The author tries to maintain a least amount of silent period for fulfilling the both purposes (location privacy, reduce the chance of accidents). The author says that if the silent period is long then it could lead to accidents. The authors compare three silent period based privacy schemes (CAPS, RSP, and SLOW) and analyze the silent period's effect using PREXT simulator.

Zhang et al. [143] suggest a "TPPR: A Trust-Based and Privacy-Preserving Platoon Recommendation Scheme in IOV" to diminish traffic congestion and raise travel comfort. The trust-based concept is used to select reliable vehicles and avoid malicious vehicles. Paillier cryptosystem and pseudonyms are used to preserve the privacy of vehicles. Trust and authentication is employed to identify the applicable vehicles. Its efficiency is better against sophisticated attacks in IOVs.

Ghane et al. [144] presented a data adaptive system known as "Preserving privacy in the internet of connected vehicles that scales the noise with respect to the data correlation". Ali et al. [145] presents "Issues, challenges, and research opportunities in ITS for security and privacy" and discuss the solutions and limitations. These issues arise in ITS due to mobile nature, high speed, sparse and dense scenarios, bandwidth limitation, decentralization, and malicious attackers. ITS security and privacy schemes are classified into group signature-

based schemes; Pseudonym based schemes and hybrid schemes. Pseudonym based schemes are further classified into symmetric and asymmetric cryptographic schemes. Moreover, the authors discussed the cloud with ITS.

Cheng et al. [146] discussed a "Location prediction model based on the IoV for assistance to medical vehicles" based on the Long Short-Term Memory (LSTM) and Deep Belief Nets (DBN). The suggested model considers driving environment, vehicle's attributes, and road information as well as the association between the factors that persuade vehicle driving behaviors and vehicle positions.

## 2.4 Intelligent System based IoV

In this section, some intelligent system such as neural network, genetic algorithm and fuzzy logic based prediction models are discussed to cope with locations, traffic congestion or vehicle's flow and other prominent challenges of IoV [147]. These proposed intelligent systems outperforms than statistical or traditional model specially pertain to urban road conditions; where randomness of the vehicle's speed, direction and their position is very high. In the paper [147] authors have claimed classification approach were more suitable for the predictions of vehicle's location. In addition, neural network were used to trained the clustering model which assist to mainly traffic status at different times.

Whereas in the paper [148], Khonen Self-Organizing Map (SOM) neural network based classification model is developed for prediction of location of vehicles. The vehicle's attributes and driving information are inputs to train the SOM neural network with same starting and destination points of vehicles. Considering the facts of IoV network, neural network were used to find the route of the vehicles and thereafter genetic algorithm optimized the route and perform the position prediction of vehicle [149]. In the paper [150], authors have proposed fuzzy logic based model to provide unified safety and health conscious referred as Bikeway in urban areas. In addition, sensed environmental data (such as noise and pollution level, UV radiation, luminosity and heat index) and statistical data

(bike path type, security data and accident data) are inputs to fuzzy logic inference system to provide a quality assist route for Bike in real cities area.

### 2.4.1. Fuzzy Logic Inference System

In 1965, Lotfi A. Zadeh of the University of California at Berkeley published "Fuzzy Sets," which spread out the mathematics of fuzzy set theory and, likewise, fuzzy logic [151]. The input of the fuzzy logic inference system for the prediction vehicle's location or traffic congestions depends upon different vehicle's information such as width of vehicles and allowing driving information in the traffic lane, road information and driving information. In addition, presented fuzzy logic inference system relates to Mamdani approach having four components: Fuzzifier, Fuzzy Inference Engine, De-fuzzifier and Fuzzy Rule Base. The block diagram of fuzzy logic inference system is shown in Figure 2.1.

The linguistic variable for prominent input parameters is divided as follows. Vehicle speed, Vehicle direction, Vehicle width, Road information includes concrete platted road or some pit holes in the roads, Traffic congestion, Driver's information, RSU such as hoarding, Camera installed to captured the accidents or any unwanted incidents and speed detections units as per as applications. In the Fuzzy Logic Inference System (FLIS) unit, all the input parameter sets are completely symbolized by its Membership Functions (MFs). These MFs simply classify the input data into sets with defined range. The input parameters can be any arbitrary real-number range, but after conversion using MFs these input parameters put into range of 0 and 1. The MFs are trapezoidal and triangular membership function is used for the above input parameters written in Equation (2.1) and Equation (2.2). In addition, other membership functions are generalized bell MFs, Sigmoid MFs and Left-Right MFs. In this thesis, we use the membership function of Mamdani type fuzzy logic toolbox as defined in MATLAB toolbox [152]. Membership function of prominent input parameters are shown in the Figure [2.2 (a-c)]. Trapezoidal membership function is used for extremes cases of input parameters and for the other reaming linguistic variables triangular membership function is used. As the rules are in fuzzy logic either generated from experimental data or heuristic

approach. Here we are using heuristic approach for generating rules in FLIS. These rules are included into the knowledge base system.

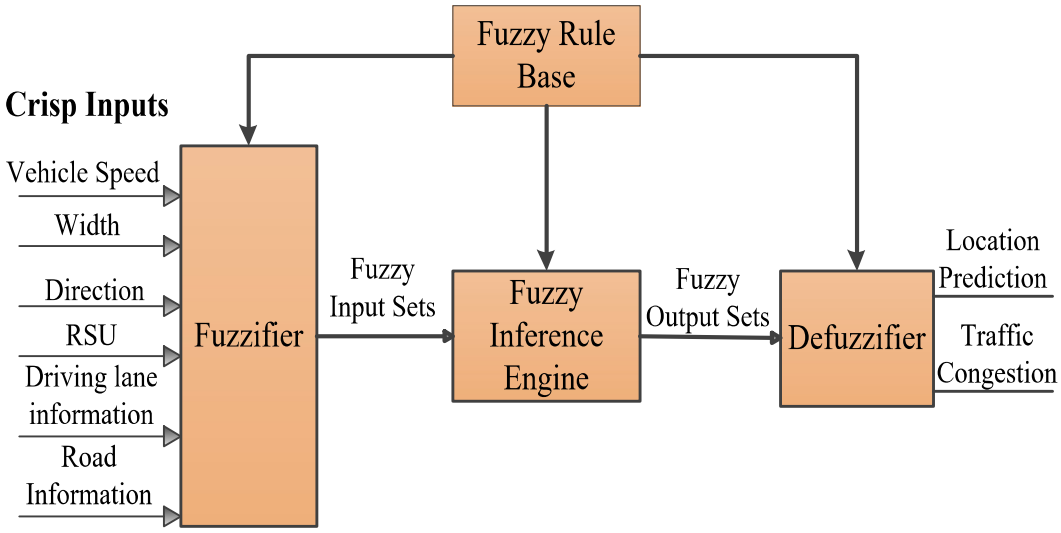



**Fig.2.1** Flow diagram of fuzzy logic inference system.

Triangular membership function is defined by three parameters $(p, q, and\ r)$ as follow:

$$\mu_A(y) = \begin{cases} 0, & y \le p \\ \frac{y-p}{q-p}, & p \le y \le q \\ \frac{r-y}{r-q}, & q \le y \le r \\ 0, & y \ge r \end{cases} = \max\left(\min\left(\frac{y-p}{q-p}, \frac{r-y}{r-q}\right), 0\right) \quad (2.1)$$

Trapezoidal membership function is defined by four parameters $(s, t, u\ and\ v)$ as follow:

$$\mu_B(y) = \begin{cases} 0, & y \le s \\ \frac{y-s}{t-s}, & s \le y \le t \\ 1, & t \le y \le u \\ \frac{v-y}{v-u}, & u \le y \le v \\ 0, & y \ge v \end{cases} = \max\left(\min\left(\frac{y-s}{t-s}, \frac{v-y}{v-u}\right), 0\right) \quad (2.2)$$

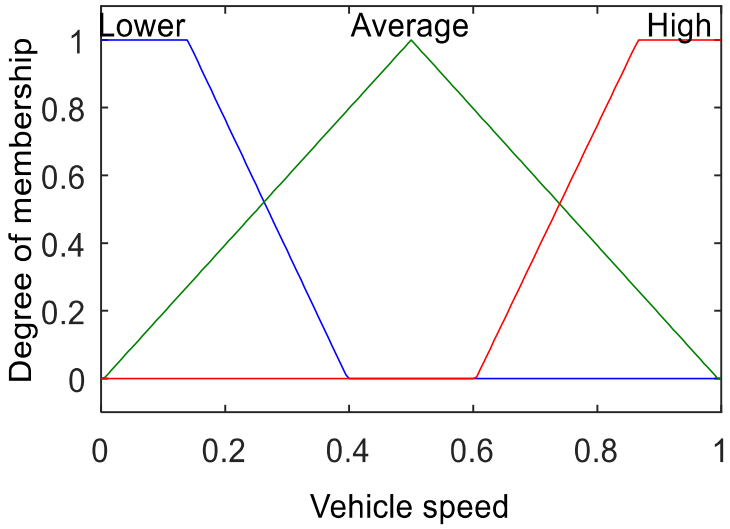



**Fig.2.2** (a) Membership functions of Vehicle speed.

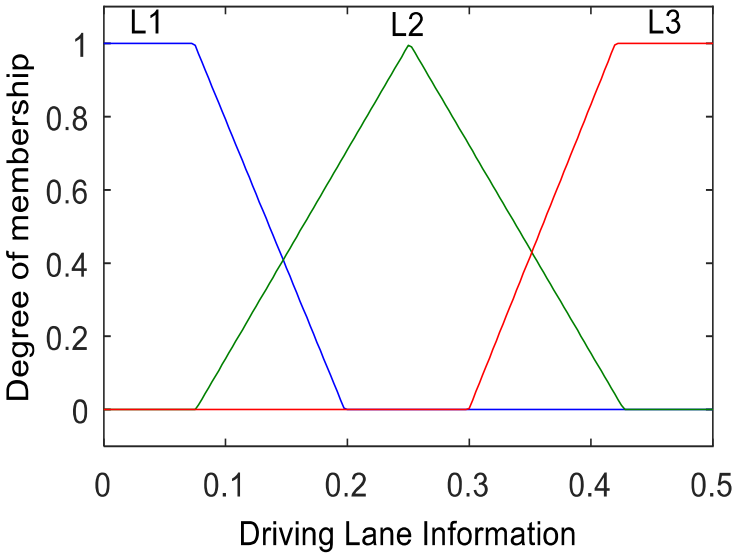



**Fig.2.2** (b) Membership functions of Driving Lane Information.

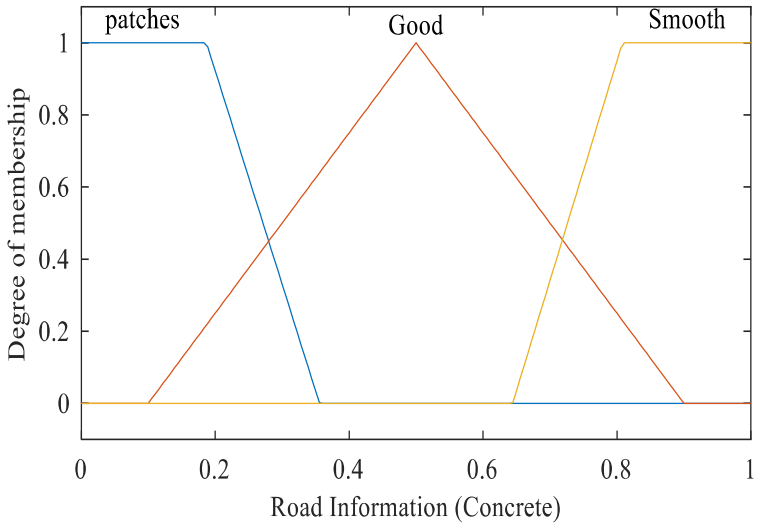



**Fig.2.2** (c) Membership functions of Road Information (Concrete).

The probability of the predicting the vehicle's location as output results in realistic environment in IoV network through FLIS is divided into seven linguistic variables shown in Figure 2.3.

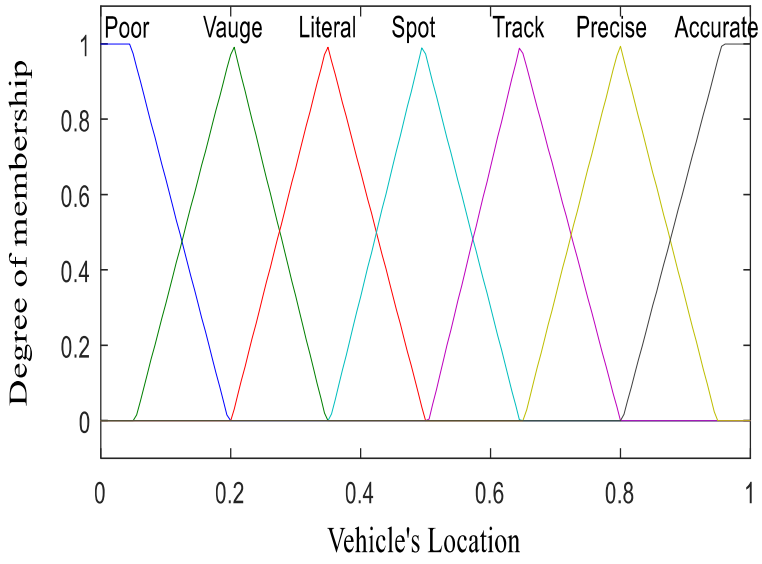



**Fig.2.3** Membership functions of Vehicle's Location as Output.

The FLIS works into four steps as follows.

**2.4.1.1 Crisp Value Input and Fuzzification**

The parameters such as vehicle speed, direction, width, driving lane information, road information and RSU are input to the fuzzier unit of FLIS. Now fuzzifier decides the range of input parameters based upon triangular membership function which is the intersection point and creates fuzzy sets or simply it converts into numerical value between 0 and 1using mathematical formula through graph function. Mathematical formulations of the fuzzification as follow.

For instance, $x_0 \epsilon\, u$ is fuzzified into $x_0$ according with the relation:

$$\mu\, x_o\, (\mathrm{x}) = \begin{cases} 1, & if\ x = x_o \\ 0, & otherwise \end{cases} \tag{2.3}$$

And an interval input $[a, b]$ is fuzzified into

$$\mu_{[a,b]}(\mathrm{x}) = \begin{cases} 1, & if\ x \in [a, b] \\ 0, & otherwise \end{cases} \tag{2.4}$$

**2.4.1.2 Fuzzy Rule Evaluation as Firing Strength**

It comprises of series of IF-THEN standards. The whole information rule runs simultaneously on fuzzy sets input in any request. Assuming any knowledge base rule is selected and fire from the dependent of fuzzy IF rules then it must be adds to the arrangement space. As though THEN have products inputs, so least choice rule AND administrator is applied to choose least among multiple input participation, and single result yield confined to the output set.

Consider a crisp input value $x_o$ with MF $\mu_{Li}^{0}$, the firing level for the Linguistic Variable $Li$ in the interval $[a, b]$ is evaluated as:

$$\mu_{Li}^{0} = \max\{\min\{\mu_{Li}^{0}(x), \mu_{[a,b]}(\mathrm{x})\} | x \in [a,b]\} \quad (2.5)$$

For a linguistic $A_i'$ variable input, firing strength of rule is evaluated as:

$$\mu_{Li}^{0} = \max\{\min\{\mu_{Li}^{0}(x),\ \mu A_i'(\mathrm{x})\} | x \in I_A\} \quad (2.6)$$

**2.4.1.3 Aggregation of All Output Rules**

As there are different output results, to collectively aggregate them into single fuzzy set OR operator is used. This operator selects the maximum number of output results and collectively placed into one fuzzy output sets.

**2.4.1.4 Defuzzification**

Deffuzification converts the output $(y)$ fuzzy set into crisp output using different methods. The most general defuzzification method is centroid method, which is often called as center of gravity or center of area given as follow.

$$y^* = \frac{\int \mu_A(\mathrm{y}) * \mathrm{y} d\mathrm{y}}{\int \mu_A(\mathrm{y}) d\mathrm{y}}, \quad (2.7)$$

Where $\mu_A(y)$ define degree of membership function of object y in fuzzy set $A$, which is defined as in terms of ordered pairs: $A = \{(y, \mu_A(y)) | \ y \epsilon U\}$ where $U$ is the universe of discourse.

**Advantage**

- It is very robust in nature.
- It is much easily implementable than its predecessors such as linear algebraic mathematical formula.
- It can adapt to the environment with little modification in the knowledge base rule.
- It can cope with multiple input and multiple output parameters.
- Time complexity in linear order and economical in nature.

## 2.4.2 Convolution Neural Network

A Convolution Neural Network (ConvNet) is feed-forward multilayer neural network introduced by Yann LeCun and Yoshua Bengio in 1995. ConvNet are used to learn useful information directly from data alias features through composition of non-linear transformation of the data [153-154]. ConvNets is supervised deep learning method shown in the Figure 2.4. It is comprised of one or more than one hidden layers (as pooling step) to take advantage of 2D/3D image of input parameters.

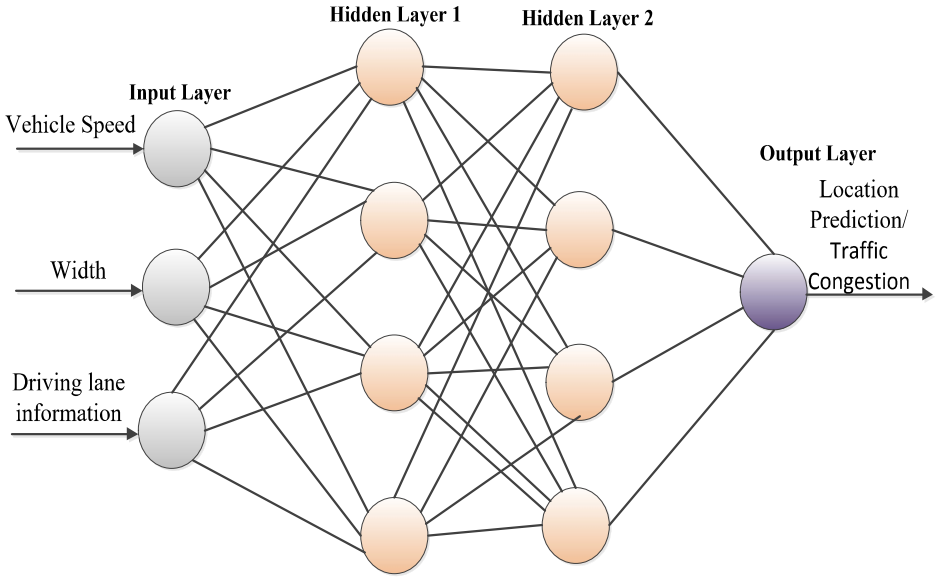



**Fig.2.4** Multilayer Perceptron: All connected ConvNet Layers.

- ***Architectures of ConvNet Layers Patterns***

ConvNet arranges their neuron in 3D (width, height and volume) anticipates as one layers shown in the Figure 2.5. The ConvNet layers mainly consist of four layers as stacked sequences. Through differential function each layers of ConvNet is transform into alternative layers shown in the Figure 2.6.

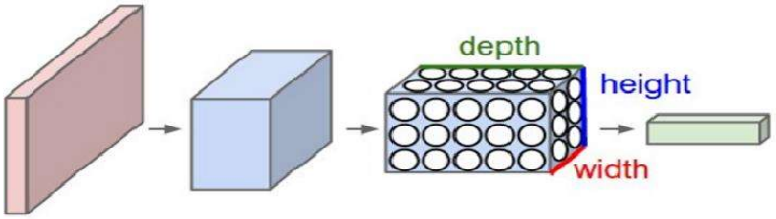



**Fig.2.5** Architecture of ConvNet layer.

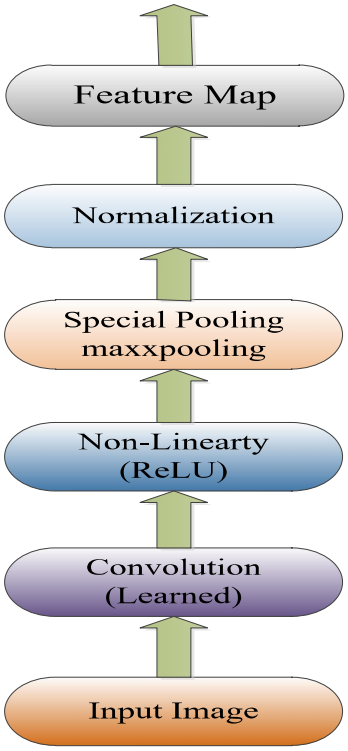



**Fig.2.6** Flow diagram of the ConvNet.

**(1)** Each ConvNet layer evaluates the output of each neuron connected to their local region. ConvNet layer requires four basic hyper-parameters i) Number of filters (k) ii) Filter's spatial exposure (F) iii) Number of stride (S) iv) Zero padding (P). Each evaluation involves dot product between weight and the local region input volume to the neuron.

**(2)** The Rectified Linear Units (ReLU) activation layers applied on each output of the ConvNet layer to provide non linearity to the system. The basic ReLU activation function

$f(x) = \max(0, x)$, this non-linear activation function changes all negative values of each element of input volumes into 0.

**(3)** After ConvNet and ReLU on the each input volume, pooling layers is applied on the output of ReLU layers. It is also called down-sampling layers which reduce the output's dimension (both width and height but depth remains unchanged) of previous layer in turn complexity in the network computation reduces as well. The basic function is max-pooling having stride of same size as filters of dimension $2 \times 2$.

**(4)** Fully-Connected (FC) layer applied to compute the class score, as output in volume of size $(1 \times 1 \times N)$. Where $N$ represents the class score of each different categories.

In others words, overall architecture of ConvNet can be describe as follow:

$$INPUT \rightarrow [[CONV \rightarrow ReLU] * N \rightarrow POOL?] * M \rightarrow [FC \rightarrow ReLU] * K \rightarrow FC]$$

Where $0 \leq N \leq 3$ and $M \geq 0, K \geq 0$

## 2.5 Privacy-Security Preserving Models

Several issues of protecting the privacy of the data in IoV have emerged in recent years and the research on analyzing such problems have been carried out in both academics and industries to make life secure. The privacy protection of the identities of the vehicle can be done effectively with the help of various authentication approaches [155]. These authentication approaches are broadly classified into three types such as cryptography-based authentication technique [156], reputation evaluation-based technique [157], and hardware-based trust enhancement technique [158]. Cryptography-based authentication technique deals only with the correct evidence holds by the vehicle. This approach neglects the reputation behavior of the vehicle. Cryptography-based authentication technique includes Identity-Based Encryption technique (IBE), Public Key Infrastructure technique (PKI), etc. On the other hand, reputation evaluation-based techniques can progressively increment or

decrement the credibility of the vehicle based on its behavior to fulfill the trust threshold verification. This is applicable for the profoundly self-organizing IoV.

**Limitations:**

- Above technique also have drawbacks of lacking robustness to the insecure vehicle in the IoV network. Lastly, the hardware-based techniques are focused on building a confided computing platform at the terminal layer for the vehicle in IoV. This is because of vehicle's reliability is controlled by monitoring the hardware unit, software unit, and other units. The hardware unit includes actuators, electronic control unit, interfaces, etc., whereas the software unit includes the operating system environment, on-board applications, etc. Here, the speed of authentication for keeping the information confidential and securely has been improved as it has self-cryptographic system. But the vehicles participating in IoV are co-related. So, security provided only to the terminal layer is not sufficient.

In the case of authentication techniques for privacy protection, several kinds of research have been carried out in recent years. The paper in [159] considers the Zero-Knowledge proof method to verify the identities. In [160], they proved that it is probably going to lessen the total unique certificates of the vehicle by distributing the certificates to their neighboring vehicles. This authentication approach deals only with identity authentication and also fails to meet the privacy of real life. To find the culprit causing a traffic accident, the true identities can be revealed by the traffic control center. To improve the efficiency of the authentication technique, researchers in academic and industries proposed to embed hardware chips into the vehicles for security purposes. Those are responsible for both data encryption and decryption carried out through hardware unit of the vehicles. It also helps to keep some private data secure. Trusted Platform Module (TPM) and Tamper Proof Device (TPD) are hardware-based authentication techniques and the comparative analysis for both the technique is demonstrated in [158].

Besides the three types of authentication technique, some other technique includes group signature and ring signature. Earlier Boneh [161] and Lin [162] developed vehicle communication based on group signature. Privacy-preserving protocol along with confidentiality in VANET based on the sign-encryption technique has been introduced by Hu et al. [163]. In the case of the group signature framework, vehicles acquired secret keys and public keys to avoid information leakage. With the increase in the number of nodes, time also increases gradually which concludes that group signature consumes an enormous amount of time. To solve this problem, the researchers adopted a solution based on the tamper-proofing of hardware devices. When the enemies attack the hardware device, the security system is compromised automatically [164-165].

In this case, ring signature was developed [166-167], Xiong et al. proposed the privacy protection protocol and ring signature technology for IoV [167]. But this requires truthful traffic management agencies. Zeng also proposed Conditional Anonymous Ring Authentication Solution (CARS) for IoV. Liu proposed an authentication technique based on session keys used in complex communication. Wu developed a secret key allocation system. It includes verification codes and establishes security by providing authentication of group keys. Recently, Hu et al. provide an efficient privacy-preserving authentication system in VANETs on the basis of ring signature [168]. They also developed an efficient, trustworthy, privacy-preserving VANETs protocol based on proxy re-signature. Besides this, they developed a protocol based on remote authentication.

**Limitations**

- Both the above discuss models have authentication techniques have the data encryption capacity, but TPD has certain drawbacks such as high price, intolerable to extreme temperature. In [158] paper, TPM was used to verify the components present in the vehicle whether they are working properly on the command without alleviating the security provides by IoV.

## 2.6 Privacy and Security Preserving using Blockchain technology

The emerging blockchain technology provide decentralized network for data storage, which provide user's (vehicles) to broadcast the information anonymously in 5G&B IoV network without worrying about their privacy in non-trustful fog (RSUs) nodes. It also helps to secure the transaction (payment) in terms of smart contract between vehicles to RSUs without using any intermediary. Recent research involves artificial intelligence and machine learning techniques into 5G&B IoV network to continuously collect the information and optimize the payment in return paid to users through learning fog node [169-170]. In the paper [155], authors have proposed deep learning reinforcement learning algorithms to motivate the users for uploading the information to the fog nodes in 5G IoV network, but lacks in privacy and security of the users.

## 2.7 Summary

Most of the data storage and authentication are constructed based on cloud computing technology. In this technology, data are stored in cloud servers by the authentication center or RSUs. Here, the assumption of cloud service providers to be reliable may not be true in real life because certain users and cloud servers may develop conspiracy. Considering the above problems, Chen et al. [171] proposed a light-weight protocol and anonymous aggregation protocol using fog computing for V2I communication schemes. Finally, after considering several security problems occurring in IoV there is need to design novel model for protecting privacy as well as keeping concerned on the security of the information in IoV.

# Chapter 3

# Video Streaming in Urban Vehicular Environments: Junction-Aware Multipath Approach

In multipath video streaming transmission, the selection of the best vehicle for video packet forwarding considering the junction area is a challenging task due to the several diversions in the junction area. The vehicles in the junction area change direction based on the different diversions, which lead to video packet drop. In the existing works, the explicit consideration of different positions in the junction areas has not been considered for forwarding vehicle selection. To address the aforementioned challenges, a Junction-Aware vehicle selection for Multipath Video Streaming (JA-MVS) scheme has been proposed. The JA-MVS scheme considers three different cases in the junction area including the vehicle after the junction, before the junction and inside the junction area, with an evaluation of the vehicle signal strength based on the Signal to Interference plus Noise Ratio (SINR), which is based on the multipath data forwarding concept using greedy-based geographic routing. The performance of the proposed scheme is evaluated based on the Packet Loss Ratio (PLR), Structural Similarity Index (SSIM) and End-to-End Delay (E2ED) metrics. The JA-MVS is compared against two baseline schemes, Junction-Based Multipath Source Routing (JMSR) and the Adaptive Multipath geographic routing for Video Transmission (AMVT), in urban VANETs.

## 3.1 Introduction

Wireless communication between moving vehicles is increasingly becoming the focus of research for both automobile companies and academic research communities [172]. It is driven by the vision that the exchange of information between vehicles can be exploited to improve the safety and comfort of drivers while in motion [173]. One of the most valuable VANETs applications is video streaming [174], which can offer more understandable and attractive on-road traffic information to drivers and passengers. The communicated video

can be related to driving safety; for example, an accident ahead, or pedestrians or animals crossing the road [175]. It can also be related to on board communications, such as V2V or Vehicle-to-Office (V2O) video conferencing [176]. On-board infotainment can also offer advertisements provided by supermarkets or shopping malls along the road utilizing roadside unit IoT environments [177]. Consequently, the video streaming service can reasonably improve the onboard experience of the vehicles. The daunting issues of video streaming in VANET are packet drop, delay and bandwidth-constrained wireless network environments [178]. This is due to the extremely dynamic topology of vehicles and the large size of video data packets sent across the wireless network [179]. These challenges become worse for high-quality video streaming, because of the even larger size of video data [180-181].

Current multimedia applications require high capacity communication links to facilitate high speed data transfer rate. Video applications require stringent video quality requirements including minimum delay, packet drop, and efficient bandwidth utilization [182-183]. Hence, there is a need for efficient video data transmission considering the characteristics of both VANETs and video streaming applications. When trying to transmit data efficiently, a path with the necessary resources to meet user requirements should be chosen. On the other hand, in conventional data networks, the routing of data is primarily concerned with an end-to-end connectivity [184-185]. The data network protocol generally represents a network with a metric such as hop-count or delay and uses the shortest path and location algorithm for path and location estimation [186]. However, in order to support the quality and delay requirements of video streaming, routing protocols usually need to take into consideration the junction area characteristics when forwarding video data [187]. The consideration of junctions on roads during transmission enhances routing decisions, achieving quality video streaming delivery [188]. A number of multipath transmission schemes have been suggested in some research studies, but few studies have considered road features such as road junctions in hop-by-hop transmission. Figure 3.1 presents vehicles in the junction area. Vehicle A, B and C are the candidate next forwarding vehicles, of which any one can be

chosen to forward a video packet. Vehicle D is the present forwarding vehicle which needs to make a decision regarding which candidate vehicle is suitable for the data packet forwarding. When forwarding a data packet in a junction area, the vehicle after the junction area with the minimum required link quality is considered to be most suitable. Afterward, the vehicle that resides in the junction with the minimum required link quality is considered as the second-best option, while the vehicle before the junction with the minimum required link quality is the third-best option.

This is because the vehicle after the junction might be closer to the targeted destination, which gives it longer connectivity and reduces the number of hops that need to be traversed. Some studies use the junction point as a forwarding area without considering the freshness of the direction of the vehicle.

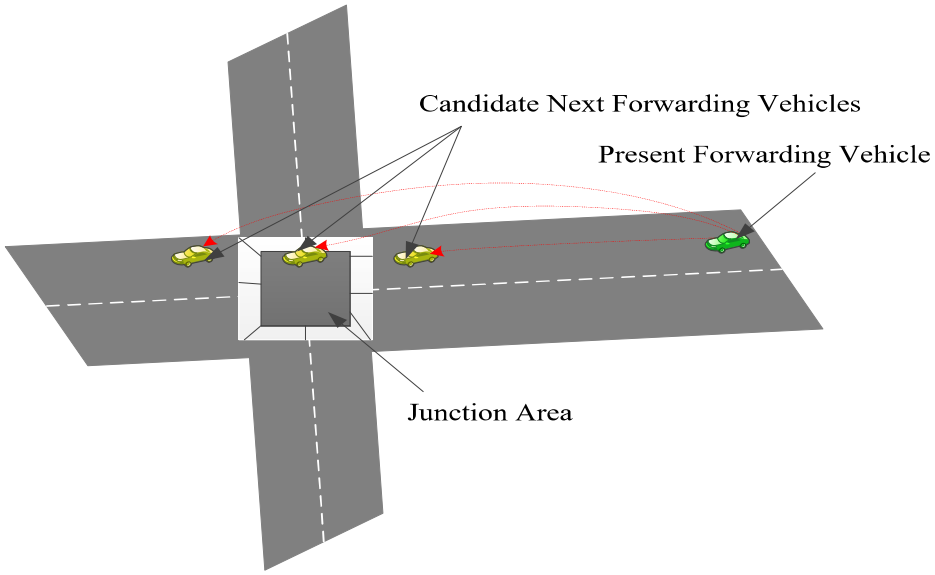



**Fig.3.1** Candidate next forwarding vehicles in the junction area.

In a junction area, the location and direction of a vehicle are essential when the vehicles' signal coverage extends to a junction area because the selected Next Forwarding Vehicle (NFV) might change its direction of navigation, which could lead to a video packet drop, thereby affecting the quality of the video streaming. Therefore, there is a need to explore the

characteristics of the junction area including vehicles that have exited the junction, vehicles in the junction and vehicles before the junction. For the video data, the video frames forwarded are split into three different frames, namely the I-frame, P-frame, and B-frame, which are forwarded via a multipath setting. The I-frames are forwarded through a dedicated path, while both P and B frames are forwarded through another path. This idea enables a higher priority for I-frames, which are the most important frames as they interpret both P and B frames.

In this chapter, we proposed a Junction-Aware scheme for Multipath Video Streaming (JA-MVS) considering different points at the junction area in order to avoid or minimize video packet error or drop. Further, mathematical formulations have been adapted to estimate the suitability of a node for data packet delivery. Precisely, the contributions of this study are highlighted as follows:

**(1)** An enhanced vehicle selection considering the different points in the junction area in order to minimize packet drop due to changes of vehicle direction in the junction area.

**(2)** Improved vehicle selection based on link quality calculation, considering the Signal to Interference plus Noise Ratio (SINR), in order not to select vehicles with high noise due to obstructing objects in the urban environment.

**(3)** The simulation and performance evaluation of the proposed scheme.

The remaining portions of the chapter are organized as follows. In the first section we describe the introduction of this chapter. In section 3.2 presents the proposed JA-MVS scheme. Section 3.3 presents the implementation and simulation results with their analysis; and finally, Section 3.4 concludes the study.

## 3.2 Junction-Aware Vehicle Selection Scheme

In this section, the proposed JA-MVS scheme is presented considering the various vehicle positions at the junction area. The multipath transmission considers the junction-aware concept in hop-by-hop transmission. The consideration of road junctions during transmission enhances routing decisions to achieve quality video streaming delivery. A number of multipath transmission schemes have been suggested in some research studies, but few studies have considered road features such as junctions in hop-by-hop transmission. Some of these studies use the junction point as a forwarding area without considering the freshness of the direction of the vehicle. In a junction area, the location and direction of the vehicle are essential when the vehicles' signal coverage extends to a junction area, because the selected NFV might change its direction of navigation, which could lead to a video packet drop, thereby affecting the quality of the video streaming. Therefore, there is a need to explore the characteristics of the junction area including the vehicles exiting the junction, vehicles at the junction and vehicles before the junction. The vehicles before the junction are considered to be the vehicles at the end of the road, which is at the traffic light. The vehicles at the junction do not have a road-ID but might be in the direction of the Destination Vehicle Node (DVN), while the vehicles after the junction have recently changed their road-ID, navigating towards the direction of the DVN. Considering the vehicles at a road junction, three cases have been considered, as stated in the aforementioned discussion.

In the first case, the vehicles which have exited the junction are preferred and considered to be vehicles that have already chosen their direction of navigation. Hence, their direction is known and probably closer to the DVN; hence they are employed as the NFVs. In the second case, a vehicle at the end of the road, which is close to the junction, is the second preferred selection area for NFVs, because a vehicle before the junction might need to wait for a traffic light; thus, its direction does not change instantly and it can be used to forward video streaming to the direction of the DVN. The third case is employed if there is no suitable vehicle that has exited the junction and no vehicle at the end of the road; then, the

vehicle inside the junction area is selected. However, the third case is only employed if the first and second cases do not occur. Therefore, in the proposed JA-MVS, the vehicles that have already exited the junction or intersection area are considered based on the freshness of their location, direction and speed information. Consequently, the JA-MVS scheme is in two stages: information exchange and a video streaming data forwarding stage in the junction area. The detailed discussion of the JA-MVS scheme is given in the next subsections.

### 3.2.1 Information Exchange Phase

At the information collection phase, every vehicle exchanges a hello message with its neighbor vehicle. The Hello Message (HM) is exchanged within a time interval of every second. The HM content includes the vehicle direction, position, ID, road-ID and hello message time-stamp. The generated hello messages are stored in a Neighbor Information Table (NIT). The NIT is updated in every time interval of the hello message exchange; that is, one second. The parameters in the NIT are recorded based on tuple since the collections of items are different. The position is based on x, y coordinates, which are centered on relative distance. The road-ID is simply an identifier which is alphanumeric. The time stamp is recorded in seconds. The direction is based on four cardinal directions including north, south, west and east. The vehicle-ID is recorded based on an alphanumeric identifier. The information packet format is depicted in Figure 3.2. The direction and position are estimated using the GPS of each vehicle, which is employed to determine the location of the vehicle in the junction area. The road-ID is used to determine if the vehicle is on the new road and is employed for the vehicle selection at the junction area. A linked list is used to store packet information, as the sizes of each element are different, with standard units considered such as milliseconds for time stamps, latitude and longitude with six-digit decimal points, etc. In addition, the selection considers the quality of the vehicle signal based on the SINR, as formulated in Equation (3.1), before considering the three cases in the junction area. In addition, the vehicle density at the junction has been considered for suitable candidate vehicle selection, which is shown in Equation (3.2). In the generic concept of the geographic

routing, the Source Vehicle Node (SVN) is already conscious of the direction and location of the DVN in the network based on the location service system and GPS. Therefore, the greedy algorithm is adapted in a way that not only selects the vehicle closer to the destination but also takes into account the aforementioned three different cases of the junction area.

$$SINR_{(p_i,p_j)} = \frac{S_{PW} F_{RD_{(p_i,p_j)}} \times l(p_i - p_j)}{\varphi + \sigma(p_j)} \tag{3.1}$$

Where $p_i$ is the sender vehicle's position and $p_j$ is the signal receiver vehicle's position. Thus, $S_{PW}$ is the transmitting signal strength, and $F_{RD}$ is the random fading between the sender vehicle and the receiving vehicle. In addition, $l$ is the distance between $p_i$ and $p_j$, while $\varphi$ and $\sigma$ denote the external noise and small short-noise of $p_j$, respectively. We have considered one direction; that is, the directions of travel of the sensor and receiver vehicles are the same. Here, it is noteworthy that the proposal will also work for the two-dimensional scenario; that is, the directions of travel of the sender and receiver vehicles could be different or in opposite directions. However, in this case, the computation will be somewhat impacted by the speed of vehicles. Consequently, both the distance and SINR are employed when selecting a vehicle in the junction area. The vehicle density is estimated as:

$$VDR = \frac{(3 \times IDVD) + ODVD}{4 \times 2Hop} \tag{3.2}$$

The next forwarding vehicle is selected based on the Candidate Next Forwarding Vehicle (C-NFV) which has the highest value of Vehicle Density of the Road (VDR). However, the Opposite Direction Vehicle Density (ODVD) is given a smaller value by multiplying it with $\frac{1}{4}$, which is three times lower than the value of the In-Direction Vehicle Density (IDVD) multiplied by $\frac{3}{4}$. This is because the vehicles moving in the opposite direction are considered not to have longer or continuous connectivity with the forwarding vehicle. This ensures that a C-NFV moving towards the direction of the DVN is given higher priority.

Thus, a threshold has been assigned as $\mathrm{VDR_{max}}$ , where the $\mathrm{VDR_{max}}$ is the estimated highest value of neighbor nodes that does not lead to congestion. Therefore, the $\mathrm{VDR_{max}}$ is set to 100 vehicles/km. We have considered a road environment with opposite lanes and assumed that 50 vehicles on both sides of opposite lanes in a 1 km road length will not result in congestion. This will result in a 20-meter road distance for each vehicle, which we consider a normal situation without congestion in urban road environments. The C-NFV case that has a greater number of vehicles than the $\mathrm{VDR_{max}}$ ($\mathrm{VDR} > \mathrm{VDR_{max}}$) is considered to be a congested network. Therefore, we obtain Equation (3.3):

$$VDR = \begin{cases} 1 & VDR \leq VDR_{max} \\ 0 & VDR > VDR_{max} \end{cases} \tag{3.3}$$

The VDR is estimated for two multiple paths independently since the paths are dispersed. The road density of a C-NFV is compared with the other road densities of the neighbor vehicles of a Candidate Next Forwarding Vehicle, and the road with the highest density, but which is not greater than the $VDR_{max}$ , is considered for selection. Therefore, the vehicle density of the road is considered to be one of the important metrics that enables optimal NFV selection. This, in turn, improves the quality of the video transmission, since the faster selection of NFV has been considered based on the density of the vehicles on the road. The most suitable node depends on the two parameters of SINR and VDR, as represented in Equation (3.4):

$$S_n = \propto (M^{SINR}) + \beta(VDR_{value}) \tag{3.4}$$

where $S_n$ represents the suitable node, $M^{SINR}$ is the maximum SINR value, and $VDR_{value}$ is the value of the vehicle density of the road. Both $\propto$ and $\beta$ are the weighting factors assigned to each of the parameters. Considering that the SINR guarantees the quality of a link, the $\propto$ is assigned a weight of 0.6, while the $\beta$ is assigned 0.4 for the vehicle density of the road; thus, the total weight is 1. Therefore, the link of the suitable node selected is considered to be the most efficient link for video data transmission. Thus, an efficient link can be formulated as represented in Equation (3.5):

$$Efficient\ link\ = {TR^{Success}}/{TR^{Total}} \tag{3.5}$$

Where $TR^{Success}$ the number of packets is successfully delivered through a link and $TR^{Total}$ is the overall attempts performed during data packet transmission.

| Position (x,y) | Road-ID | Timestamp | Direction | Vehicle-ID |
|---|---|---|---|---|

**Fig.3.2** Information packet format.

### 3.2.2 Video Data Forwarding Phase

In this section, the Junction-Aware Multipath Video Streaming concept is discussed considering geographical routing; specifically, the greedy forwarding concept is adapted by modifying some of its concepts. As mentioned in the previous section, firstly, the SINR and VDR of each neighbor vehicle are evaluated based on Equation (3.1) and (3.2).

Below mentioned Algorithm 3.1, presents the procedure involved in video data forwarding when a C-NFV is in the junction area. The vehicle mobility information is gathered considering line 2. Line 3 checks if the C-NFV is in the junction area; that is, whether the C-NFV is before the junction, inside the junction or after the junction. Then, the SINR is computed considering the three scenarios of the junction area in line 4. However, the vehicle with the highest SINR value is preferred if it has not exited the junction area, as for the remaining cases of the scenarios. Thus, the SINR value selection has a higher priority than the different positions in the junction area. Lines 5-7 check if the C-NFV's road-ID is ahead of the junction location and if it has a higher signal strength value, and the optimal C-NFV—that is, the RVN—is selected. Lines 8–11 choose the first two RVNs ($P_2$ and $P_3$), whose I-frames are forwarded via $P_2$, and the B and P frames are forwarded through $P_3$.

$P_2$ and $P_3$ are the first two relay nodes before the other intermediate nodes in the two paths. The suitable RVNs are the nodes with the maximum efficient link, selected using Equation

3.5. Lines 12 and 13 check if the C-NFV is at the end of the road, which is at the traffic light. This C-NFV is selected if there is no C-NFV after the junction location towards the DVN. Line 14 forwards the video data via the RVN as previously discussed. Otherwise, the C-NFV is checked if its location is inside the junction, meaning a C-NFV with no road-ID, and this is selected if there is no vehicle after the junction or inside the junction based on lines 16–18. Otherwise, the algorithm checks whether the DVN belongs to the set of the CNFVs: if true, the video data is forwarded to the DVN and terminated; otherwise, it is forwarded to NFV based on lines 19–26.Line 27 terminates the whole procedure of the algorithm. Figure 3.3 shows the flow of the algorithm. As previously stated, the complete routing concept is based on the greedy-based geographic routing protocol. The implementation process, including the simulation setup and performance evaluation of the proposed JA-MVS scheme, has been presented in Section 3.3.

## 3.3 Performance Evaluation

In this section, the simulation setup results obtained and the performance evaluation with analysis against the baseline schemes are presented. The performance is evaluated considering two different cases. Each based on vehicle density and video data rates. The evaluation is conducted by considering metrics including the Packet Loss Rate (PLR), Structural Similarity Index (SSIM) and End-to-End Delay (E2ED).

The PLR is the ratio of a transmitted video packet to that of the delivered packet. This also helps in ascertaining the quality of the video transmitted, because the lower the number of video packets dropped, the higher the number of video packets delivered at the destination vehicle, which in turn leads to higher video quality [189]; conversely, the higher the number of video packets dropped during transmission, the lower the number of received video packets at the destination vehicle, which leads to lower video quality. The SSIM is computed as the perceived similarity between the transmitted video images and the original video images.

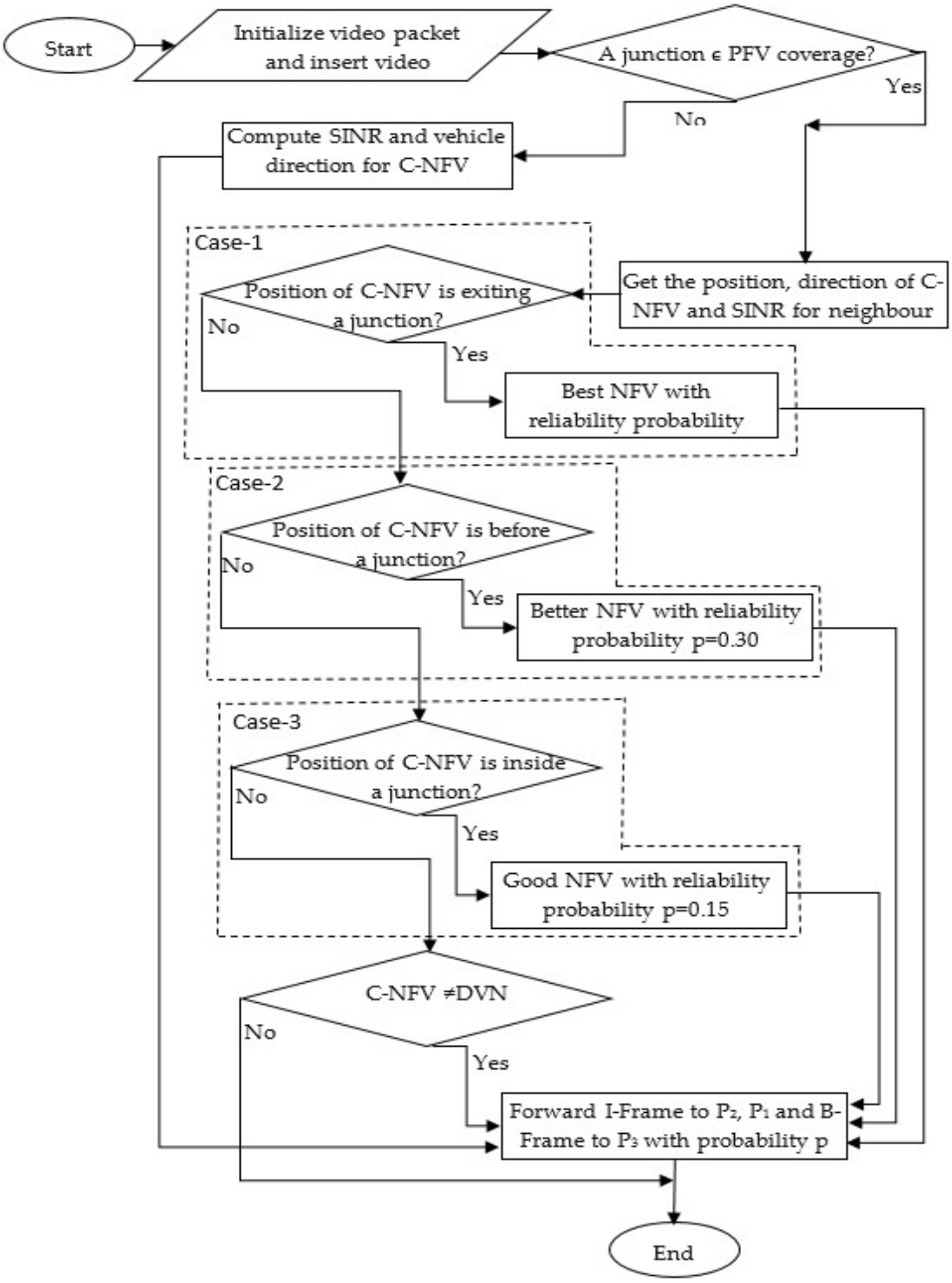



**Fig.3.3** Flowchart for vehicle selection considering the junction area.

The calculation of the SSIM index is grouped into three aspects: contrast, luminance, and structural assessment [190]. The E2ED is the total summation of the delay encountered from the source vehicle to the destination vehicle. The delay includes the propagation delay, transmitting delay, processing delay and startup delay [191-192]. The level of E2ED delay also signifies the quality of the video delivered at the destination vehicle. The metrics are tested in relation to different vehicle densities and data rates (kbps). The distribution of the vehicle density is from 50 to 500, and the video data rate considered ranges from 160 kbps to 1600 kbps.

The three metrics are utilized considering the different vehicle densities and data rates. Particularly, a high data rate and high vehicle density have been considered. The discussion of the results of the proposed scheme is presented in Section 3.3. The baseline schemes employed for the benchmarking of the proposed scheme includes Junction-Based Multipath Source Routing (JMSR) [130] and Adaptive Multipath geographic routing for Video Transmission (AMVT) in urban VANETs [131]. The simulation of the junction-aware scheme is guaranteed since the whole map of the simulation environment, including roads and junctions, has been integrated using the Open Street Map (OSM) and integrated into the Simulator of Urban Mobility (SUMO). The vehicles know their positions due to location information service.

The proposed JA-MVS is implemented using the most acceptable network simulators: NS-2.34 and SUMO. The NS-2 is a network simulator that enables the simulation of network communication. The SUMO employs the Mobility Model generator for VANETs (MOVE). It has the ability to create a realistic model for the mobility of vehicles in urban traffic scenario. The Evalvid has been employed to provide video frames and a video quality evaluation framework. The Manhattan city digital map with latitude of 39.191 to 39.184 and longitude of -96.574 to -96.563 is employed for the mobility and traffic environment setup (see Figure 3.4). The digital map structure and data are acquired from the OSM contributors.

**Algorithm 3.1** Junction-Aware Multipath Video Forwarding

***Initiatialize***: $videopktid$

***Initiatialize***: $video\ packet$

***Insert***: $videopkttp = I\_frame, P\_frame, B\_frame$

***Insert***: $ID\ of\ DVN\ when\ forwarding\ videopkt$

***Output***: $Forward\ videopkt\ from\ SVN\ to\ DVN$

***Begin*** $VideoDataForwardingat\ Junction\ area\ (p_i, data)$

  ***Obtain*** $C-NFV's\ speed, vehicle\ id, road\ id, direction, timestamp, position$

  ***If*** $the\ PFV\ is\ at\ junction\ area$ ***Then***

    ***Compute*** $SINR\ and\ VDR\ of\ C-NFV$

    ***Else If*** $C-NFVs\ position == junction\ exited$ ***Then***

      $vehicle\ exit\ junction = vehicle\ with\ new\ roadid$

      ***Locate − and − Forward()***

    ***Else If*** $C-NFVs\ position == vehicle\ before\ the\ junction$ ***Then***

      $vehicle\ before\ Junction = vehicle\ at\ the\ traffic\ light$

      ***Locate − and − Forward()***

      ***Else If*** $C-NFVs\ position == vehicle\ inside\ the\ junction$ ***Then***

        $vehicle\ inside\ junction = vehicle\ with\ no\ roadid$

        ***Locate − and − Forward()***

        ***Else If*** $C-NFV == DVN$ ***Then***

          ***Forward***$(videopkt)\ to\ DVN\ without\ SINR\ and\ VDR$

        ***Else***

          ***Forward***$(videopkt)\ to\ NFV$

        **Exit**

        ***End if***

      ***End if***

    ***End if***

  ***End if***

***End if***

***End***

**Locate-and-Forward ()**

1. ***Identify*** *theNFV with higher SINR and VDR*
2. ***dentify*** *suitable two RVNs from SVN for* $P_2$& $P_3$ ↔ *conditions*
3. ***Forward*** *videopkttp*$(I_{frame})$& *videopktid to NFV via* $P_2$
4. ***Forward*** *videopkttp*$(P\_frame, B\_frame)$ *to NFV via* $P_3$

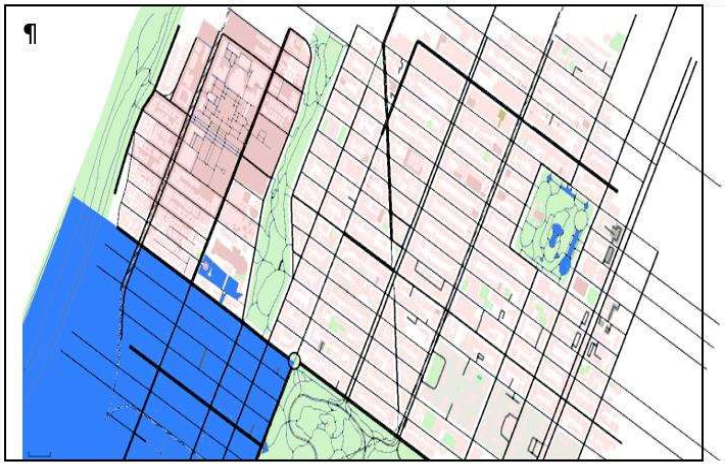


**Fig.3.4** Manhattan city map.

The details of the simulation parameters are depicted in Table 3.1, which include the urban simulation area, simulation time, vehicle speed, number of vehicles, the Medium Access Control (MAC) protocol, video resolution, video play duration, the transmission range, frequency bandwidth, propagation model, antenna model, traffic type, channel type, transmission protocol, hello packet timeout and scenarios.

## 3.3.1 Results Analysis of the JA-MVS Scheme

The results obtained for the performance analysis of the proposed scheme in comparison against the baseline schemes are presented here. Figure 3.5 (a) and 3.5 (b) shows the performance improvement of the JA-MVS scheme against the two baseline schemes of JMSR and AMVT.

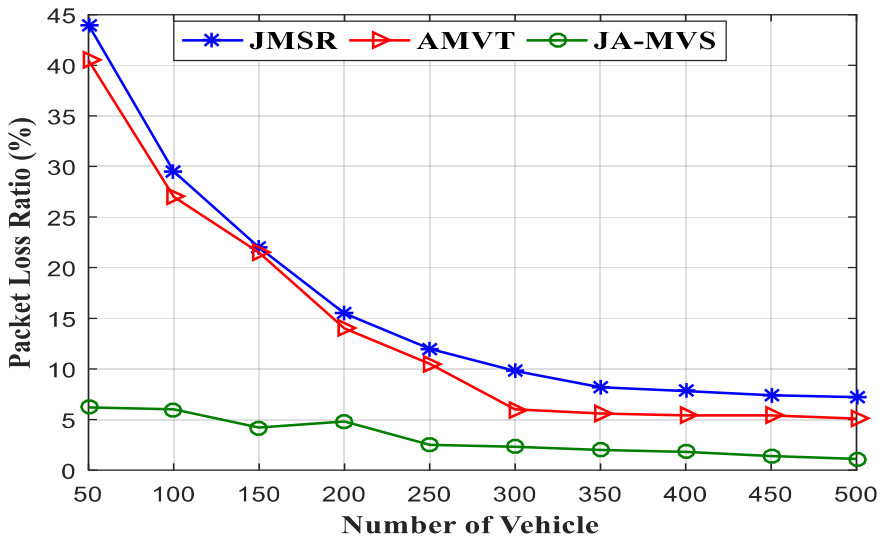
Figure 3.5 (a) shows the performance of the schemes based on PLR against different vehicle densities. It is observed during the simulation results that the number of dropped video packets decreases as the vehicle density increases. The two baseline schemes experience more than 40% video packet drop when the vehicle density is 50; this is due to the consideration of only junctions as nodes in the case of JMSR.

**Table 3.1** Simulation parameters.

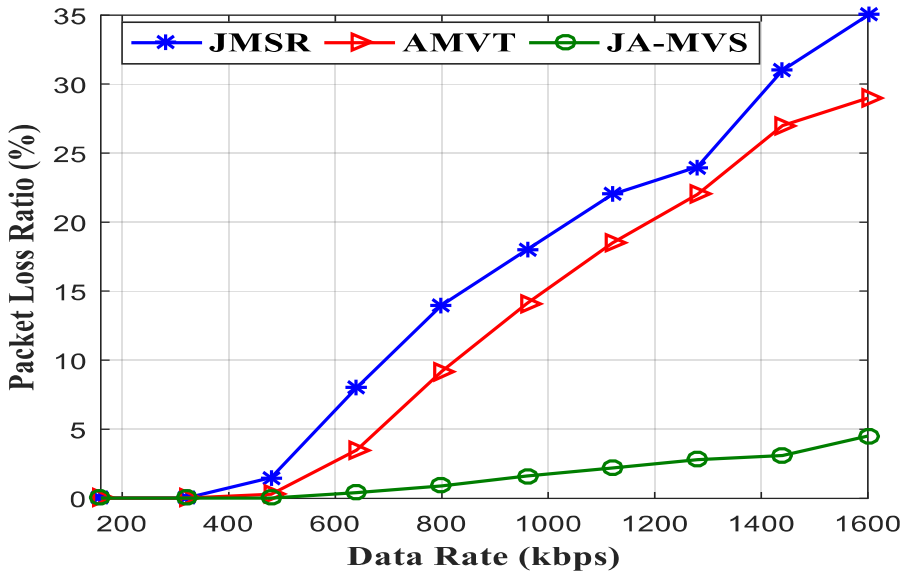
| **I. Parameters** | **II. Values** |
|---|---|
| III. Urban simulation area | IV. 1000 × 1000 $m^2$ |
| V. Simulation time | VI.600 s |
| VII. Vehicle speed | VIII. 2.78 to 13.89 m/s (10 to 50 km/h) |
| IX. Number of vehicles | X. 50 to 500 |
| XI. MAC protocol | XII. IEEE 802.11p |
| XIII. Video resolution | XIV. 352 × 288 |
| XV. Video play duration | XVI. 139 s |
| XVII. Transmission range | XVIII. 250 m |
| XIX. Frequency Bandwidth | XX. 5.9 GHz |
| XXI. Propagation model | XXII. Shadowing |
| XXIII. Antenna model | XXIV. Omni-directional |
| XXV. Traffic type | XXVI. Constant Bit Rate |
| XXVII. Channel type | XXVIII. Wireless |
| XXIX. Transmission Protocol | XXX. UDP |
| XXXI. Hello packet timeout | XXXII. 1 second |
| XXXIII. Scenarios | XXXIV. High-density urban scenario |
| XXXV. Comparison protocol | XXXVI. JMSR and AMVT |
| XXXVII. Metrics | XXXVIII. PLR, SSIM index and E2ED |

The high PLR encountered for the AMVT is related to the building obstruction model used to detect obstructions before sending a video packet to the next forwarding vehicle. The obstruction detection might not be realistic due to the frequent position changes of the vehicle; thus, the vehicle continues carrying packets for some period of time, which are later dropped.

However, as the vehicle density increases, there is a higher number of vehicles to be selected as NFVs with better link quality for video packet transmission. Further, with higher density, the two baseline schemes have lower PLR values, which are below 10%, even trending towards 5%. Nevertheless, the proposed JA-MVS scheme performs better at 7.5% PLR at 50 numbers of vehicles, with the PLR becoming lower than 5% when the vehicle density is 150. The better performance of JA-MVS is connected to the consideration of junctions, which is based on three different cases: the selection of vehicle that has exited the junction that is before the junction and inside the junction, with its navigation being towards the direction of the DVN. With the aforementioned considerations, the proposed scheme outperforms the two baseline schemes. The average percentage packet losses experienced by JMSR, AMVT, and JA-MVS are 16.3%, 14.4%, and 3.4%, respectively.




(a)




(b)

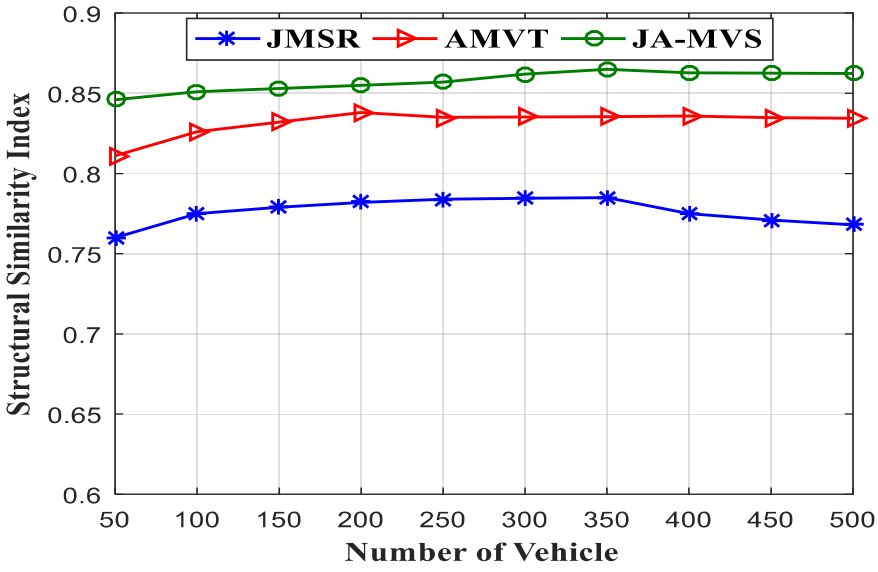
**Fig.3.5** Packet Loss Ratio based on (a) Varied vehicle densities and (b) Data rates.

The performance improvement of the video packet loss by JA-MVS with a density of 50–500 vehicles against the JMSR scheme is 12.9% and that against the AMVT scheme is 11%. Hence, the proposed JA-MVS performs better in terms of the video packet loss ratio.

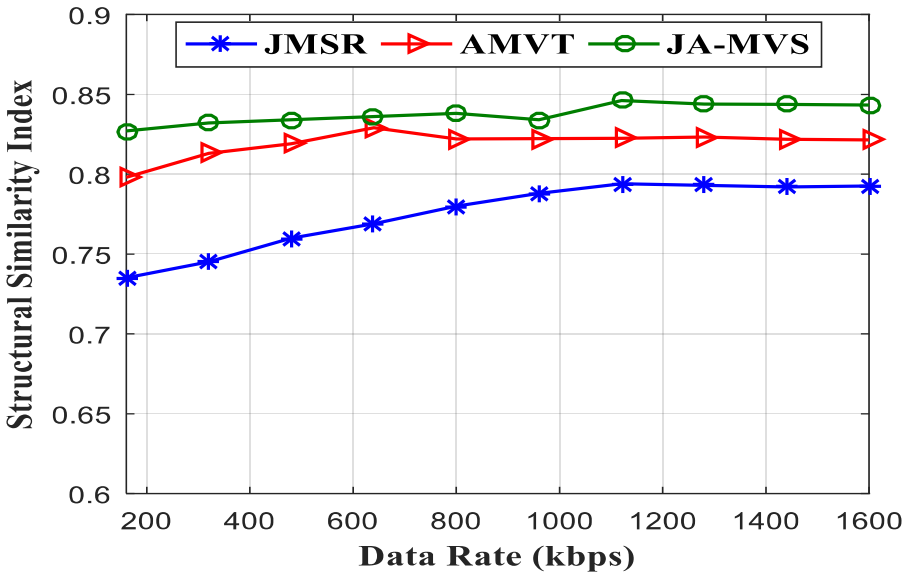
Figure 3.5 (b) depicts the results of the PLR studied alongside the various transmitted data rates. The results show that the packet loss ratio increases as the data rate increases. At 160 to 320 kbps, there is no loss of video packetw experienced; however, a packet loss starts to manifest when the data rate is 400 kbps. The packet loss increases above 30% for JMSR and AMVT schemes as the data rate increases. However, the highest packet loss experienced for the proposed JA-MVS scheme is 5.5% when the data rate is at 1600 kbps. Therefore, the JA-MVS outperforms the two baseline schemes. The better performance achieved by the proposed scheme is related to the reliable selection of NFV based on the direction and position of the C-NFV at the junctions of the road. The aforementioned considered parameters have helped in attaining successful video packet delivery with fewer packet losses. The average percentage gains of the three schemes are 15.4%, 15.5% and 2.1% for

JMSR, AMVT, and JA-MVS, respectively. The average percentage gains of the performance of JA-MVS against JMSR and AMVT are 13.3% and 13.4%, respectively.

The SSIM is measured as a value between 0 and 1; the results are presented in Figure 3.6 (a) and 3.6 (b) accordingly. Figure 3.6 (a) depicts the results obtained based on the SSIM index of the video transmission in relation to various vehicle densities. Based on the results obtained, the SSIM index increases gradually for both the three schemes as the vehicle density increases. The highest video SSIM index values were observed when the vehicle density is between 300 and 350. For the JMSR scheme, the SSIM index increases gradually until it starts to decline when the vehicle density is above 350; however, despite the fall in the video quality, the result is above the average value of the SSIM index of 0.5. Further, the SSIM index of the AMVT scheme also gradually increases as the number of vehicles increases; the increase almost became static with a small increase when the number of vehicles was 200 to 500. The SSIM index of the proposed JA-MVS scheme increases based on the increase in vehicle density. The proposed JA-MVS scheme performs better than the two baseline schemes in terms of the SSIM index.




(a)




(b)

**Fig.3.6** Structural Similarity Index based on (a) Varied numbers of vehicles and (b) Data rates.

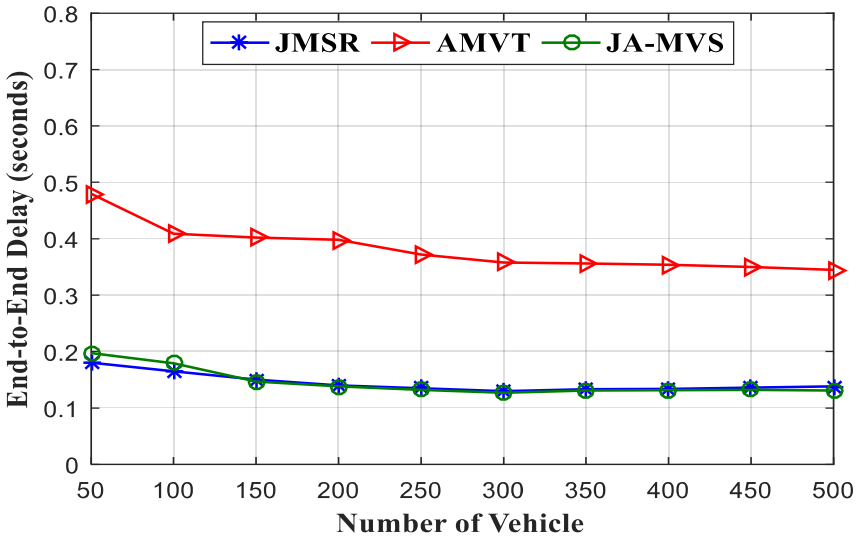
The observed increase in the SSIM index is connected to the approach used for the selection of the NFV in the junction area of the road. This approach avoids the drop of video packets because vehicles that are not moving towards the DVN and that do not have the required link quality are not considered. In addition, the approach avoids the occurrence of loops or local maxima as opposite direction vehicles are avoided, except in the case of the non-availability of a vehicle in the direction of the DVN. Consequently, the results show that JA-MVS outperforms both JMSR and AMVT. The percentage gains of the three schemes are 77.6%, 81.0% and 84.7% for JMSR, AMVT and the proposed JA-MVS schemes, respectively. The average percentages of performance improvement of the JA-MVS over JMSR and AMVT are 7.1% and 3.7%, respectively.

Figure 3.6 (b) depicts the results of the SSIM index based on different video data rates. The different data rates of transmission are employed in order to show that the proposed scheme has the ability to make a fast NFV selection for video data transmission without encountering a large queuing of video data packets at the receiver vehicle. The result of the

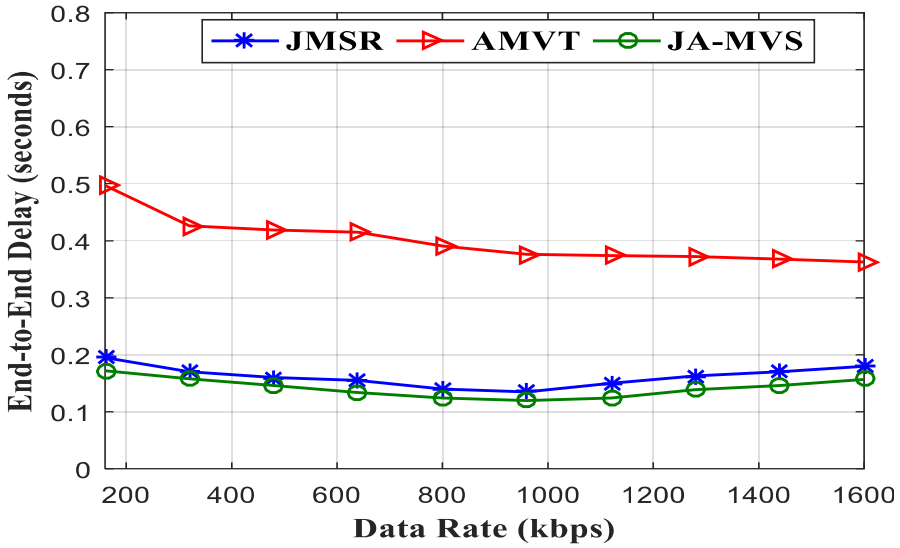
experimentation demonstrates that the value of the SSIM index increases as the transmitted data rates increases for all the three schemes. The increase in the value of the SSIM index reaches its peak when the data rate is above 1000 kbps and below 1400 kbps.

The SSIM index value tends to decline when the data rate is above 1400 kbps. However, the values of the SSIM index for each of the schemes are above average value, which is 0.5. Further, as observed from the results, the proposed JA-MVS performs better than both JMSR and AMVT.

The improved performance can be related to the comprehensive selection procedure which includes all three different cases of the junction area, which provides a faster and more current status of vehicle position before selecting a vehicle as an NFV. Considering the selection, video traffic due to video queuing is minimized; hence, there is little or no traffic of video data. Considering the results, the proposed JA-MVS scheme outperforms the two baseline schemes. The average percentage gains of the three schemes are 77.5%, 80.1% and 84.0% for JMSR, AMVT, and the proposed JA-MVS, respectively. The percentages of the performance improvement of JA-MVS against JMSR and AMVT are 6.5% and 3.9%, respectively.




(a)




(b)

**Fig.3.7** End-to-End Delay based on (a) Varied numbers of vehicles and (b) Data rates.

The E2ED is studied alongside different densities of vehicles and data rates, which are shown in Figure 3.7 (a) and 3.7 (b), respectively. Figure 3.7 (a) demonstrates that both JMSR and JA-MVS have lower transmission delay in contrast with AMVT. The E2ED has been plotted alongside different densities of vehicles. A high delay is experienced in AMVT considering the fact that more than two routes have been considered, which can lead to the severe collision of video packets due to route coupling, thus causing a delay in video packet arrival time. Although, the JMSR also encountered a little delay, it is lower than that of AMVT. The result of the E2ED of JMSR is almost the same as that of the proposed JA-MVS scheme. This is connected with the fact that there is frequent signaling during communication between all neighbor vehicles. In video streaming, the delivery of data packets with few losses is more important than a delay of ≤5 seconds being experienced, because the loss of packets affects the quality of the video streaming. Thus, there is a balance in the tradeoff between cost and performance. Meanwhile, the overall delay experienced for the two aforementioned schemes is minimal. Therefore, the JA-MVS scheme outperformed the JMSR with only a small marginal difference. The JA-MVS

performs better than the AMVT scheme because the proposed scheme employed different junction area situations to select the best forwarding vehicle towards the DVN. It also continues transmission through the selected NFV except if the vehicle is no longer in the neighborhood of the PFV. The percentage of E2ED encountered is computed considering the maximum allowable delay of 5 seconds. Thus, the JA-MVS, JMSR, and AMVT schemes obtain values of 2.7%, 2.9%, and 14.0%, respectively. The percentages of performance improvement of the JA-MVS against JMSR and AMVT are 2.0% and 11.3%, respectively.

Figure 3.7 (b) depicts the E2ED results plotted alongside different data rates in order to assess the performance of the proposed scheme. The proposed JA-MVS has the lowest delay compared to both the JMSR and AMVT schemes. The high delay experienced in AMVT is connected to the high data rate transmitted, which causes queuing of video packets at the transmitting vehicle because of route coupling, which causes a collision. The JMSR and the proposed JA-MVS schemes have an almost equal delay. However, JMSR encounters higher video packet loss. Nevertheless, JA-MVS outperformed the JMSR scheme because it takes into consideration junctions with vehicles moving in opposite directions in the case of the non-availability of a vehicle in the direction of the DVN. The proposed scheme performed better than the AMVT because JA-MVS employs only two paths for the video streaming forwarding, while AMVT utilizes more than two paths, which leads to video packet collision. The average percentage delay encountered is considered based on the maximum allowable delay of 5 seconds. The JA-MVS, JMSR and AMVT schemes obtain values of 2.9%, 3.2%, and 10.9%, respectively. The percentages of performance improvement of JA-MVS against JMSR and AMVT are 0.3% and 8.0%, respectively.

## 3.4 Summary

In this paper, a junction-aware vehicle selection strategy for multipath video streaming in a vehicular network has been proposed. The JA-MVS scheme transmits video packets considering the different positions of the on-road junctions and the SINR as the signal quality for best forwarding vehicle selection. In the junction-aware algorithm, a vehicle that

is ahead of the junction and moving toward the DVN is given higher priority to establish reliable video packet forwarding in the junction area. The SINR is an important metric for evaluating vehicle signal strength considering the urban scenario, which has a lot of obstacles that affect vehicle signal during transmission. The simulation results validate that the JA-MVS scheme significantly improves the video transmission performance in relation to the increase in quality of the video streaming, with a lower PLR and higher SSIM and a decrease in the overall E2ED of the video packet transmission. In addition, the simulation shows that the overall performance of the JA-MVS outperformed the two baseline schemes of JMSR and AMVT. Moreover, to further extend the proposed scheme, future research should focus on different kinds of roads including highway bridges and bent roads, considering their effects on video data packet forwarding to achieve quality video streaming in VANETs.

# Chapter 4

# An Efficient Lightweight Authentication Scheme for VANETs

With the rise of the number of vehicles on the road and smart city idea, VANETs have been generally known for vehicle communication to get information of traffic congestion, speed, road condition location of the Vehicles etc. Generally the urgent task of the researcher is that how the data are securely transmitted between the vehicles in the VANETs. For VANETs many of the privacy-preserving authentication protocols have been developed but they have lots of computation and security issues. Privacy and authentication is the most important part of VANETs since various attacks such as location tracking, identity revealing and authentication, steal sensitive information to create considerable risk for human day to day lives. The attacker changes confidential information such as speed, direction, path, location of vehicle, speed, road condition information, traffic congestion description and exploits its privacy. The existing privacy-preserving schemes like pseudonym schemes, anonymous signing protocol, group signature, and authentication-based schemes, mix zone and silent period, etc. are inefficient in terms of storage, privacy-preserving, and implementation. Furthermore, they impose high overhead and converges very slowly. To remove the issues mentioned above of existing privacy-preserving schemes in VANETs, we suggest an authentication protocols to ensure security of the passenger privacy which uses only Exclusive-OR (Ex-OR) operations and hash functions, a lightweight authentication protocol in a suitable communication design for VANETs that meets the privacy protection needs. The proposed method not only integrated authentication, but also keeps the vehicles secret. Furthermore, we simulated and then compared our schemes to other relevant schemes to determine its efficiency and performance. Its provide better performance as compare to the others schemes also comparing our protocol to other relevant protocols reveals that it is more suited to real world environments.

## 4.1 Introduction

Smart homes and smart cities have stimulated the interest of nations and governments all over the world in recent years [137]. The main motivation is to improve people's quality of life. With the help of communication and information technology, IoT [193] and WSNs [194-196], the smart city idea is progressively becoming a reality and life of citizens upgraded because of infrastructure and facilities. By using these techniques like medical care, traditional transportation, and waste management etc. could be greatly improved. It is undeniable that the city's vehicle population is growing day by day and the ITS has emerged as an essential technology for managing city traffic, with VANETs [197] which is providing assistance for road safety.

The On-Board Unit (OBU) in VANETs is a tamper-proof device which is installed in a vehicle that can hold the vehicle's vital secret information, such as its identity and some cryptographically generated results. The system also includes a Trusted Authority (TA) and a large number of Road Side Units (RSU). The RSUs are mounted on the side of the road and serve as a communication link between the vehicles and the TA. The TA is providing support for any essential communication services as well as responsibility of vehicles and RSU registration. In VANETs, there are two modes of communication which is V2I and V2V. Formally vehicles directly communicate with each other when it is with in the certain range later its communication is done with the help of RSUs that means the message is firstly send to the nearest RSUs after that is delivered to the vehicles. DSRC is used by both V2I and V2V communication [9] that is helped for increasing the transportation safety and efficiency. V2I appears to be a promising way [198] for VANETs applications nowadays.

Due to a drastic increment in the number of automobiles on the road, several traffic critical issues such as accidents and threats are increasing. VANETs consists of Mobile Nodes (MNs) that are embedded in vehicles and linked in a self-organized way to transmit information among vehicles and RSU [137]. It is used for high-level road safety applications, optimized traffic management where data exchange is possible with the help of

V2V and V2I wireless communication. During V2V communication, vehicles available in the communication range are communicated to share road conditions and traffic information for reducing the chances of a severe accident. Since it is used in safety-critical applications (safety of vehicle drivers and passengers), the security protocol must include privacy, availability, data consistency, authentication, traffic congestion, and non-repudiation [199-200]. ITS [201] are built on top of VANETs. It resolves traffic-security associated issues by combining communication technologies with traffic information for efficient and secure communication of information. VANETs improves the responsiveness of various traffic-related events. VANETs Nodes (VNs) are classified as OBU and RSU. OBU are the radio devices installed on vehicles, and RSU are placed along the roadside to constitute the network infrastructure as well as controlled by a network operator. Since large scale VANETs uses dynamic ad-hoc network topology with fast-moving vehicles, the existing secure communication protocols are ineffective.

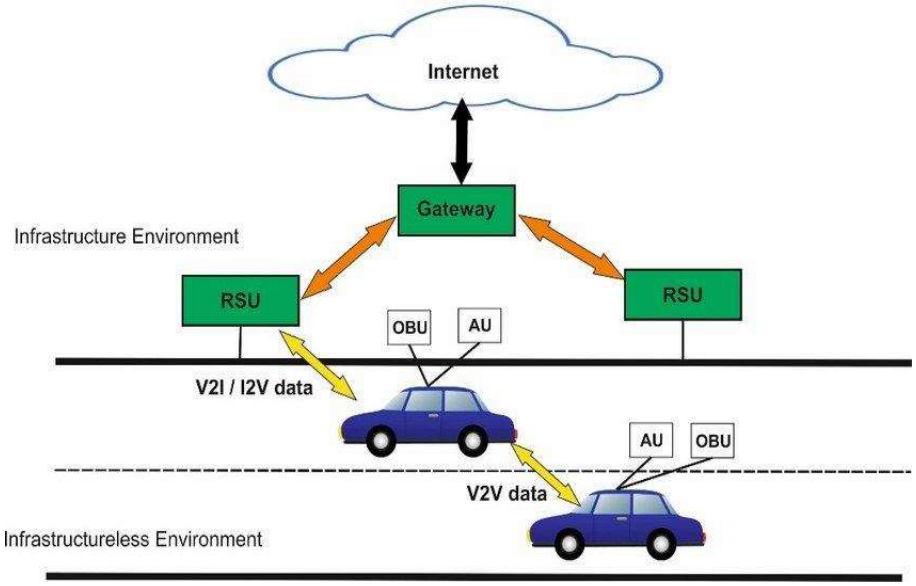



**Fig.4.1** General VANETs system.

VANET-specific communication protocols seem to be an effective solution for vehicular environments since they efficiently provide crucial traffic information, accident sites and

road conditions to alleviate the accident problems. The protection allied application protocols in VANETs are "WSMP by WAVE, CALM FAST by ISO, and C2CNet by C2C consortium". Vehicular communications facilitate traffic management and improve the traveling experience with navigation with a high risk if no security measurement is considered. Wireless Access in Vehicular Environment (WAVE) is the admired architecture of VANETs provided by IEEE [201-202]. The main purpose of the attack on Privacy is identity revealing and location tracking. The several privacy preservation schemes such as anonymous signing protocol, group signature scheme, digital signatures, mix zone method, and random encryption periods, etc. to achieve Privacy in VANETs are developed.

Figure 4.1 shows the design of broad VANETs system. The characteristics of VANETs include high mobility, driver safety and optimized traffic flow, direct interaction of vehicles with each other, vulnerable to attacks due to dynamic network topology, recurrent network disconnection, no power constraint, and limited transmission power. Several researchers have discussed various security and location privacy schemes for VANETs [203-204]. Researchers are interested in developing security and location privacy schemes for VANETs since it enhances road safety and optimize traffic flow by transmitting various Safety Messages (SM) among vehicles. The robust security algorithms will provide the driver and passenger safety with security services such as authentication, availability, data integrity, privacy, and nonrepudiation [205]. VANETs properly utilizes the communication system and vehicle resources to reduce traffic congestion as well as limit (control) the unlikable events caused by severe traffic accidents.

Figure 4.2 lists the major advantages, challenges, and applications of VANETs. Due to the high mobile nature of VANETs, security, and Locations Privacy (LP) are the most critical challenges since it is vulnerable to various kinds of security threats [206-207]. However, we provide a list of VANETs attacks and their defense techniques using Figure 4.3, but some uncovered greedy behaviors need to be resolved to improve security [208-210]. These attacks affect the functioning of other applications, degrade the security level, and malfunction comfort applications. The attacks on the VANETs communication are privacy

attack, eavesdropping attack and certificate replication attack. Moreover, the attacks on safety applications are DoS attack, jamming attack, betrayal attack, and platooning attack. These attacks are related to channel allocation. There are two types of attacks in VANETs: insider attack and outsider attack [211-213]. Insider attacks cannot be detected and defended by cryptographic solutions. Trust-based security solutions are an efficient way to catch such insider behaviors. However, cryptographic solutions can defend external attacks very well with some computational overhead [214].

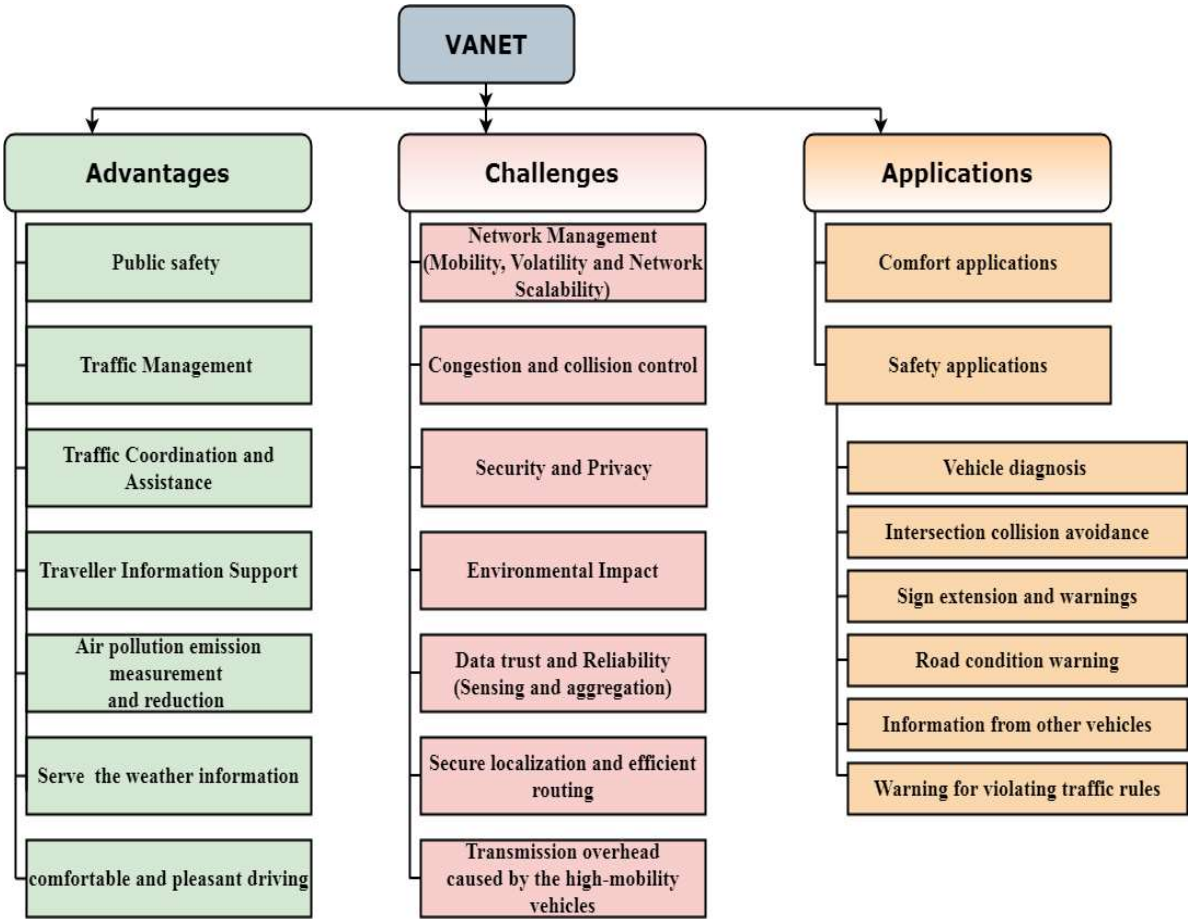



**Fig.4.2** Advantage, Challenges and Applications of VANETs.

In VANETs, the vehicle location and user identity are not closed, and vehicle LP can be tracked by unregistered vehicles. To maintain the vehicle security and privacy (ID, location),

pseudonyms are being used effectively [215]. However, vehicle location plays a vital role in VANETs since all other applications and associated algorithms work after obtaining traffic-related information from vehicles [216]. Furthermore, access control is also a challenging issue in VANETs for which various levels are predefined. Data exchange and data security are also important issues since they require many resources and broadcast sensitive safety messages [217]. These communication messages provide safety in locating and tracking vehicles and creating a location privacy risk in the dynamic Adhoc environment. For efficient communication, sensitive safety messages should not be altered by the attacker. In case if the attacker changes the private information, it should be detected as soon as possible to minimize the risk. An attacker changes it behavior to disturb the VANETs for personal benefits [218-219]. The process of illegitimately getting private information of vehicles is called an attack on privacy. These attacks are classified as identity revealing and location tracking [220]. It affects driver privacy and puts passengers at risk since vehicles and drivers are related to each other. The main purpose of these attacks is automobile thefts or abductions. To avoid such risks of unauthorized location tracking, the transmitted message containing sensitive information must include verifiable identity and other accurate data. There are various location privacy schemes such as anonymity-based approaches, policy-based approaches, and regulatory approaches [221,146]. Each approach has some merits and demerits.

The remaining work is divided into three more sections; namely, in the section 4.2 network model is propose further in the section 4.3 projected location authentication schemes is discussed and the proposed work further divided into four phases in the first phase we discussed the system initialization phase, second one is RSU registration phase, third one is vehicles registration phase and lastly the authentication phase. In section 4.4 we informally compare our proposed scheme with the already existing authentication schemes. At last, we summarize the paper and provide the future scope of the work.

| Security attacks and their countermeasures in VANETs | | |
|---|---|---|
| **Attack type** | **Compromised services** | **Countermeasures** |
| DOS | Availability, authentication | Use the bit commitment and signature-based authentication technique |
| Jamming | Availability | Use frequency hopping technique, direct-sequence spread spectrum (DSSS) |
| Malware | Availability | Reliable hardware and digital signature of software |
| Broadcast tampering | Availability, integrity | Cryptographic primitives are enabled for prevention, but a nonrepudiation mechanism may exist |
| Blackhole, grayhole | Availability | Reliable hardware and digital signature of software |
| Eavesdropping | Confidentiality, integrity | Exploit physical layer security protocols |
| Traffic analysis | Confidentiality | Use encryption techniques |
| Man-in-the-middle | Authentication, confidentiality, integrity | Robust authentication technique such as digital certificates |
| Sybil | Availability, authentication | Deployment of central validation authority (VA), location and position verification |
| Tunneling | Integrity | Reliable hardware and digital signature of software and sensors |
| Message tampering | Availability, authentication | Zero-knowledge schemes for authenticate message |
| Replay | Authentication, integrity, nonrepudiation | Message authentication, using digital signature scheme |

**Fig.4.3** VANETs attacks and their defense techniques.

## 4.2 Network Model

Figure 4.4 show the network model for the VANETs employed in this section, which is made up of RSUs, TA, and vehicles. TA has enough memory and computational capability and it is trustworthy; RSU has less memory and computational capability as compare to TA and also not entirely trustworthy; OBU is a temper proof device which is mounted on the vehicle, it is away from data extraction, generally used for securing the data. Vehicle has less memory and computational capability as compare to the RSU and TA. In this model, authentication message is send by the vehicle to the nearest RSU which is forwarded to the TA. Wired (stable) medium are used between TA and RSU while wireless medium (Like DSRC) are used between the RSU and vehicles. We use the simple technique to reduce the updating problem of the group that all vehicles transmitted the data to the RSU closest to them, and only the relevant RSU and vehicles shares a session key such as signature based protocols [222-223]. OBU mounted on the one of the vehicle has a problem and not able to transmit the information then accident will have no impact on the group's communication. Moreover, before the session key can be determined, the three participants in the VANETs must complete mutual authentication, so that RSU and vehicles must receive the message from TA. In IoT also the same kind of communication round is used for authentication.

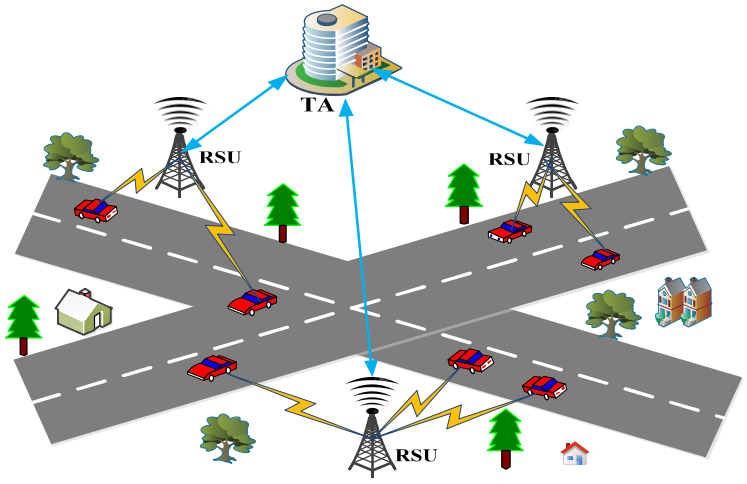



**Fig.4.4** Network model.

## 4.3 Proposed Work

### 4.3.1. System Initialization Phase

The following steps define the system initialization phase:

- TA chooses a random number $r \in \mathbb{Z}^*$ as secret key.
- TA chooses a one-way secure cryptographic hash function $h(.): \{0,1\}^* \rightarrow \{0,1\}^l$.

**Table 4.1** Symbols and their meaning.

| **Symbol** | **Meaning** |
|---|---|
| RSU | Road-side unit |
| OBU | On-board unit |
| $TA$ | Trusted authority |
| $V_i$ | $ith$ vehicle |
| $R_j$ | $jth$ RSU |
| $N_{V_i}$ | Random number generated by $V_i$ |
| $N_{R_j}$ | Random number generated by $R_j$ |
| $ID_{V_i}$ | Identity of $ith$ vehicle |
| $PID_{V_i}$ | Pseudo-identity of $ith$ vehicle |
| $ID_{R_j}$ | Identity of $jth$ RSU |
| $SK_{RSU}$ | Secret key of RSU |
| $SK_{TA}$ | Secret key of TA |
| $k$ | Shared secret key between $R_j$ and TA |
| $h(.)$ | One-way secure cryptographic hash function |
| $T_{V_i}$ | Current time-stamp of $V_i$ |
| $\|\|$ | Concatenation operator |
| $\oplus$ | XOR operator |

### 4.3.2 RSU Registration Phase

The following steps define the RSU registration phase:

- TA generates an identity $ID_{R_j}$ for RSU $R_j$.
- TA chooses a shared secret key $k$ between $R_j$ and TA.
- The pair of $(ID_{R_j}, k)$ can be stored in the database of TA.
- $(ID_{R_j}, k)$ can be also submitted to $R_j$ over a secure communication channel.

### 4.3.3 Vehicle Registration Phase

- TA generates an identity $ID_{V_i}$ for $V_i$ and stores it in the database of TA.
- TA chooses $PID_{V_i}$ as pseudo identity and computes the messages $\alpha$, $\beta$ and subsequently sends $(\alpha, \beta, ID_{V_i}, PID_{V_i})$ , to $V_i$ over a secure communication channel.

$$\alpha_1 = h(r \parallel PID_{V_i})$$

$$\alpha_2 = h(r \parallel ID_{V_i})$$

- At the end, $V_i$ stores $(\alpha, \beta, ID_{V_i}, PID_{V_i})$ on the vehicle's proof tamper OBU.

### 4.3.4 Authentication Phase

Figure 4.5 shows the mutual authentication among participating entities such as Vehicle $(V_i)$ Road-side Unit $(R_j)$, and Trusted Authority (TA). The authentication steps are given below:

**Step 1:** Initially, a vehicle $V_i$ generates a random number $N_{V_i}$ and gets timestamp $T_1$. Thereafter, $V_i$ computes the following messages:

- **Compute:** $\beta_1 = h(\alpha_1 \parallel T_1) \oplus ID_{V_i}$
- **Compute:** $\beta_2 = h(\alpha_2 \oplus N_{V_i})$

- **Compute:** $\beta_3 = h(ID_{V_i} \parallel PID_{V_i} \parallel N_{V_i} \parallel T_1)$

Then, Vehicle $V_i$ sends $Msg_1 = \{\beta_1, \beta_2, T_1\}$ to the RSU $R_j$ via a secure channel.

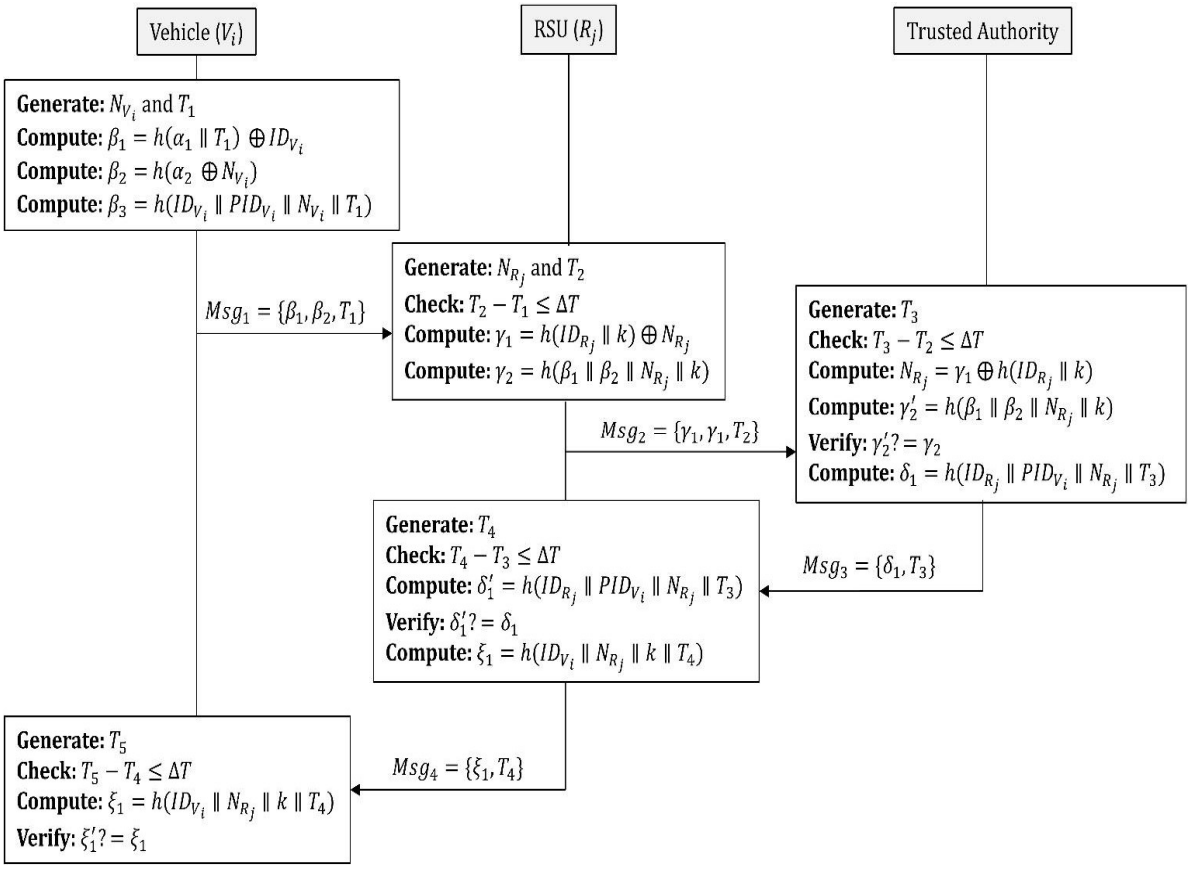



**Fig.4.5** Authentication protocol for VANETs.

**Step 2:** Upon receiving, the RSU $R_j$ generates a random number $N_{R_j}$ and gets timestamp $T_2$. The $R_j$ checks whether $T_2 - T_1 \leq \Delta T$ and computes the following messages:

- **Compute:** $\gamma_1 = h(ID_{R_j} \parallel k) \oplus N_{R_j}$
- **Compute:** $\gamma_2 = h(\beta_1 \parallel \beta_2 \parallel N_{R_j} \parallel k)$

Then, RSU $R_j$ sends $Msg_2 = \{\gamma_1, \gamma_1, T_2\}$ to the Trusted Authority (TA) via a secure channel.

**Step 3:** After receiving, the Trusted Authority gets a timestamp $T_3$ and checks whether $T_3 - T_2 \leq \Delta T$ and computes the following messages:

- **Compute:** $N_{R_j} = \gamma_1 \oplus h(ID_{R_j} \parallel k)$
- **Compute:** $\gamma_2' = h(\beta_1 \parallel \beta_2 \parallel N_{R_j} \parallel k)$
- **Verify:** $\gamma_2' ? = \gamma_2$
- **Compute:** $\delta_3 = h(ID_{V_i} \parallel PID_{V_i} \parallel N_{V_i} \parallel T_1)$

Then, Trusted Authority (TA) sends $Msg_3 = \{\delta_1, T_3\}$ to the RSU ($R_j$) via a secure channel.

**Step 4:** Upon receiving, RSU ($R_j$) gets a timestamp $T_4$ and checks whether $T_4 - T_3 \leq \Delta T$ and computes the following messages:

- **Compute:** $\delta_1' = h(ID_{R_j} \parallel PID_{V_i} \parallel N_{R_j} \parallel T_3)$
- **Verify:** $\delta_1' ? = \delta_1$
- **Compute:** $\xi_1 = h(ID_{V_i} \parallel N_{R_j} \parallel k \parallel T_4)$

Then, RSU ($R_j$) sends $Msg_4 = \{\xi_1, T_4\}$ to the Vehicle ($V_i$) via a secure channel.

**Step 5:** After receiving, Vehicle ($V_i$) gets a timestamp $T_5$ and checks whether $T_5 - T_4 \leq \Delta T$ and computes the following messages:

- **Compute:** $\xi_1 = h(ID_{V_i} \parallel N_{R_j} \parallel k \parallel T_4)$
- **Verify:** $\xi_1' ? = \xi_1$

## 4.4 Informal Security Analysis

The informal security analysis of the proposed protocol has been analyzed by comparing several existing authentication protocols for VANETs.

**Table 4.2** Comparative assessment of authentication protocols.

| Protocols | [224] | [225] | [226] | Proposed |
|---|---|---|---|---|
| Resists replay attacks | ✓ | ✓ | ✓ | ✓ |
| Resists Man-in-the-Middle attacks | ✓ | ✗ | ✓ | ✓ |
| Resists impersonation attacks | ✓ | ✓ | ✓ | ✓ |
| Resists physical attacks | ✗ | ✗ | ✗ | ✓ |
| Resists de-synchronization attacks | ✓ | ✓ | ✓ | ✓ |
| Resists cloning attacks | ✗ | ✗ | ✗ | ✓ |

## 4.5 Summary

In this chapter, we suggested a novel LAP for VANETs in which TA chooses a shared secret key $k$ between $R_j$ and TA, it is stored in the database of TA. We proposed an informal security analysis for authentication, in which we demonstrated that our suggested system meets all VANETs security standards. The proposed method not only integrated authentication, but also keeps the vehicles secret. Furthermore, we simulated and then compared our schemes to other relevant schemes to determine its efficiency and performance. Its provide better performance as compare to the others schemes also comparing our protocol to other relevant protocols reveals that it is more suited to real world environments. VANETs help in enhancing road safety and optimize traffic flow by transmitting various safety messages among vehicles .In future, we will assess the performance of the presented method using simulator in mobile environment. Moreover, we will add trust concept to improve security along with privacy. Also in future we will concentrate on network function virtualization techniques for vehicle-to-everything applications in 5G, security and privacy issues in 5G, edge computing-supported vehicle-to-everything (V2E) services, such as authentication of protocols for SDN.

# Chapter 5

# Blockchain Based Intelligent Incentive Enabled Information Sharing Scheme in IoV

With the advancement of vehicle's traffic information processing and communication capability in IoV network widely used for the vehicle-to- infrastructure transportation communication. Firstly, the protection of the user's (vehicles) privacy at the time of information sharing and secondly, users lack the motivation to share the traffic information with RSUs are two major concerns in the IoV networks. In this regard, we propose a novel Adaptive Neuro-fuzzy based Payment using Blockchain (ANFPB) transportation communication scheme that not only motivates users to take participate in the information sharing problems with the payment mechanism but also allows users to anonymously share the traffic information with RSU in the IoV network. Meanwhile, a smart contract is presented to generate pseudonyms to share the traffic information anonymously in a non-trustful IoV network. Also, an algorithm ANFPB is presented for the evaluation of payment based on location, timeline, and quality of information shared by the vehicles.

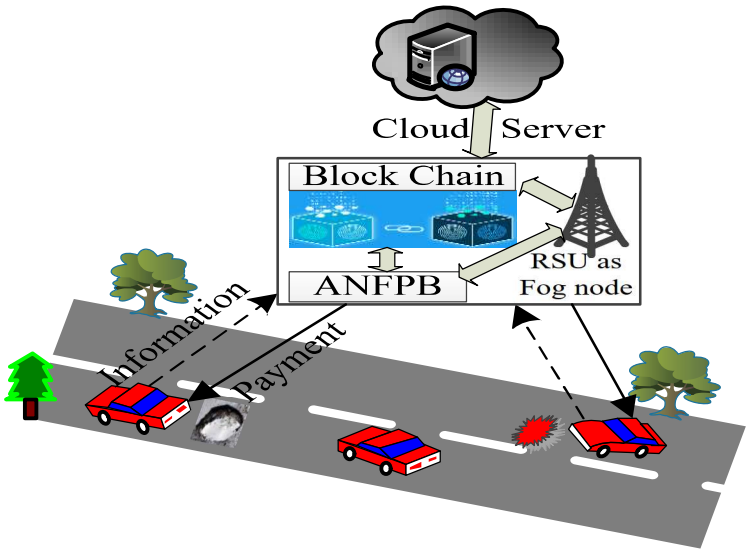



**Fig.5.1** Overall architecture of the proposed model.

Finally, the extensive simulation analysis shows that the proposed ANFPB is more efficient in terms of preserving privacy and computational costs as compared to state-of-the-art schemes.

## 5.1 Introduction

In the recent decades, more number of smart vehicles connected to the next generation internet which terms as 5G and beyond (5G&B) IoV [227-228]. This 5G&B IoV have decentralized network configuration with three layer architecture. The bottom layer corresponds to vehicles-to-vehicles communication. The middle layer responsible to V2I (RSUs) edge (fog) communications that collects the information's from the vehicles to maintain the traffic rules and avoid road hazards. The upper layer is cloud server that provides huge data storage for longer term to deep analytics in all spatial regions. 5G&B IoV network is mainly designed in such a way that it provides driving comfort and safety for the user's terms as infotainment application and safety applications respectively [229]. Non-safety infotainment applications include the real-time traffic information while driving, music on the road, video on demand, and the internet of the wheel. Whereas safety applications applicable to various domains such as alleviating highway turbulence, man oeuvre control, cooperative cruise control, traffic congestion, offenses, broken pavement, dangerous driving and accidents, weather conditions, or any looting or terrorist attack [230-231]. It requires V2I communication to frequently accessible the safety applications by the users in 5G&B IoV network. Privacy information of the vehicles such as location and identities in V2I communication and lack in the enthusiasm to take users to participate are two major issues in the establishing 5G&B IoV network.

5G&B IoV uses wireless technologies that arises privacy issues on the information's broadcasting [232-233]. Normally, data are transmitted by a vehicle to the fog node (RSUs) layer that includes the detail of user's personal information locations, travelling route. Recent literatures show that untrusted fog node reveals the user's information for money that leads to serious vulnerabilities to the society [233-234]. Therefore, preserving the privacy of

each vehicle and to ensure their integrity and authentication are other issues in the 5G&B IoV network. In case of security purposes, the identity authentication technique is the most effective approach to protect the integrity, privacy confidentiality, and availability of the data in IoV [235]. Whereas, authentication along with key exchanging technology, PKI systems is also widely used in other fields, including mobile cloud networks, smart grid, IoV network etc. [236-238]. Above literatures suffers from workload leads to a high packet loss in the case of locations with heavy traffic and only provide threshold privacy protection and not able to correctly reply to message of users. Which in turn lose to motivate the users to take participate in the V2I communication in 5G&B IoV network.

The emerging Blockchain technology provide decentralized network for data storage, which provide user's (vehicles) to broadcast the information anonymously in 5G&B IoV network without worrying about their privacy in non-trustful fog (RSUs) nodes. It also helps to secure the transaction (payment) in terms of smart contract between vehicles to RSUs without using any intermediary. Recent research involves artificial intelligence and machine learning techniques into 5G&B IoV network to continuously collect the information and optimize the payment in return paid to users through learning fog node [239-240].

In [241], authors have proposed deep learning reinforcement learning algorithms to motivate the users for uploading the information to the fog nodes in 5G&B IoV network, but lacks in privacy and security of the users. Ensuring the success of blockchain and fog-cloud technology based on artificial intelligence approaches this paper neuro-fuzzy learning algorithm to secure the information during transmission and privacy of vehicles and motivates vehicles by providing incentives to them. The clod-server provides unlimited resources for data storage and it submitted the data in such a way that not even the government agencies or law enforcement can destroy the privacy of the witness by tracking. Besides all the above importance, it is also necessary to attract the attention of the users towards this service. As aforementioned by the above challenges, privacy and attracting users' attentions towards to get the reward in exchange for uploading the information (images/video, etc.) of the site of interest (labeled as witness service by users) at the

fog-cloud 5G&B IoV network are the main purpose of this paper. In this regard, this paper presents a novel scheme ANFPB using blockchain ensuring the privacy of the vehicles, and a further adaptive neuro-fuzzy technique is used to evaluate reward based on location, timeline, and quality of the information shared by the vehicles. The major contributions of the proposed model as follow:

**(1)** Firstly, a system model, network model, and blockchain technology are presented to define the involved physical entity, fog-cloud network layer for information sharing and to ensure privacy and provides the reward to users respectively in 5G&B IoV network.

**(2)** Secondly, we briefly define the system initialization process, pseudonyms exchange mechanism for privacy-preserving that include smart contract on blockchain to ensure the authenticity of the vehicles.

**(3)** Thirdly, a novel Adaptive Neuro-Fuzzy Payment based on Blockchain (ANFPB) is presented to evaluate the reward for the vehicles based on the shared traffic information. Further, to make the scheme free from fraudulent users' revocation authority revokes the vehicles based on their pseudonym exchange history table.

**(4)** Finally, performance evaluation is presented to compare the privacy and computation cost of the proposed model concerning state-of-art-models.

The chapter is organized as follows. Section 5.2 discusses the details of the system model, network framework with blockchain structure. Section 5.3 describes the proposed model. Section 5.4 explains the details of presented ANFPB algorithm. The performance evaluation and the comparison of the proposed model and the state-of-art models have been shown in section 5.5. Finally, this chapter is concluding in the section 5.6.

## 5.2 System, Network, and Blockchain Model

### 5.2.1 System Model

The proposed system model is the association of IoV and fog-assisted cloud computing technology. Active participants of this model consist of vehicles (sensor nodes) equipped fully with IoV infrastructure such as DSRC based On Board Unit (OBU), cameras, Tamper Resistant Hardware (TRH), Department of Motor Vehicles (DMV), Revocation Authorities (RAs), Law Enforcement Organization (LEO) and judiciary. The above mention participants are the physical participants in the system model. Further, fog assisted cloud computing technology is employed to store the information collected through road-side cameras and process this information for forensic investigation purposes.

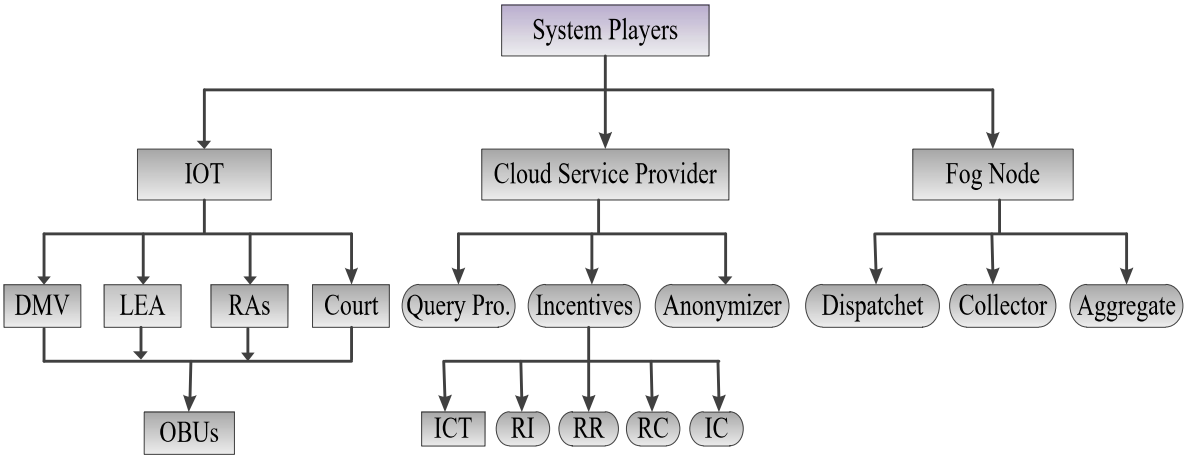



**Fig.5.2** Architecture of System Model.

Finally, this processed information is handed over to the judiciary as evidence of the events. In the case of cloud computing, the storage of the information is done in two layers as fog layer and the cloud layer. Fog layer is used to collect the data; aggregate the data, anonymized the data, and dispatch the data. Here, RSUs is considered as fog node. It is mainly used for storing instant data in turn latency in uploading the information reduces by the virtue of fog layer. In addition to that, loss of captured information is less as the report

(images/text file/audio/video) of an event can be stored in multiple fogs. Whereas, cloud infrastructure responsible for storing all the information, processing the related query, data dispatching, and rewarding systems. Further, it also analyses the information for forensic investigation, taking necessary precautionary measures whenever required or generates a warning message.

Furthermore, the cloud provides details of forensics data to trustworthy agencies, including government agencies, law enforcement agencies, judiciary, insurance agencies, etc. To encourage user participation on the road, we proposed Privacy Assure Rewarding System (PARS) for providing reward to the vehicle based on the contribution as services. Rewarding systems consist of one physical entity known as Reward Collection Centre (RCC). This Centre can be petrol pump, gas station, post office, zoo, food court, etc. This physical entity also consists of other software modules such as receipt collector, receipt receiver, receipt issuer, and reward calculator. The arrangement of the participants in the system model has been depicted in Figure 5.2 above.

### 5.2.2 Network Model

The proposed network model has been illustrated in Figure 5.3. This model describes the process of transferring the captured information through the on-board cameras of vehicles to the nearest RSUs using DSRC. The information can be any events such as accidents, traffic jams, terrorist attacks, etc. of the Site of Interest (SoI). The data are aggregated in the Fog (RSUs) layer and send to the cloud layer by remotely triggering. In our proposed work, we used passive service which includes several cameras either installed in the vehicles or on the road side to capture images of the SoI and transfer it directly to fog layer with low latency and suitable to store instant information. Later it is transferred to the cloud layer with high security using the blockchain technique. These data are kept in the cloud layer for future purposes where it can be used for the forensics investigation process. This information is also used to avoid the terrorist attack, destructive events, deadly accidents, etc.

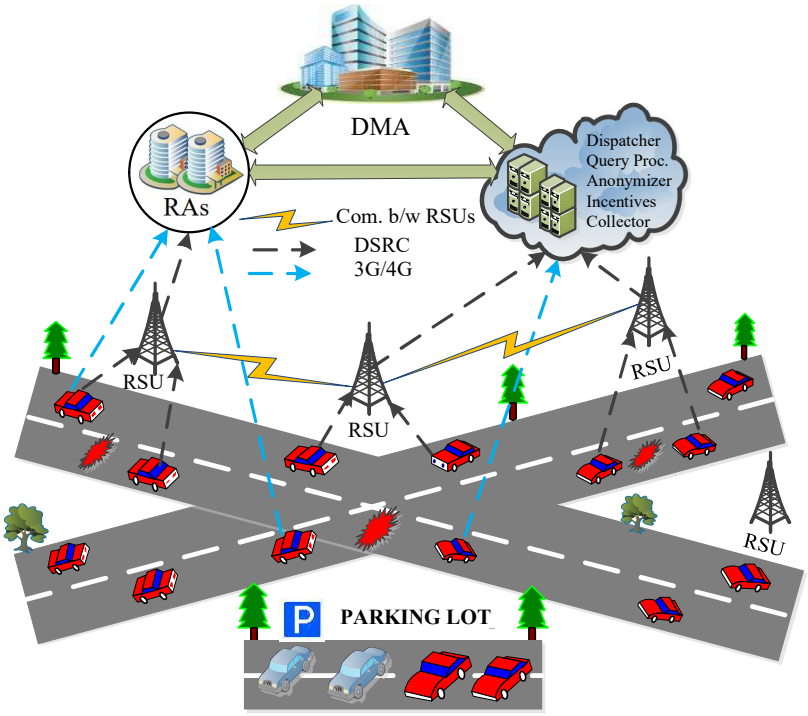



**Fig.5.3** Proposed Network Model.

### 5.2.3 Blockchain Structure

Blockchain was proposed in 2008 by Satoshi Nakamoto and has become an effective technology with a significant impact of decentralizing the business way. Blockchain is defined as a synchronized and disseminated record keeper in terms of listing blocks. On considering, its immutable and distributed data storage technique, blockchain is applicable to various areas such as banking, health care, supply chain management, trade finance, a transaction in IoT network, etc. The advantage of blockchain is depicted in Figure 5.4. In the public blockchain structure, there is no central manager involved instead of the participants in the network is responsible for maintaining the public record. Systematically, in public blockchain, anyone can add a new block by Proof-of-Work (PoW) mechanism, which is a cryptographic puzzle technique. A node that determines the solution to the puzzle disclosed the solution to all other nodes present in the network. While nodes will accept the solution only when there is a validation of all the transactions occurring in new blocks. Beforehand,

it needs to be confirmed that no other solution has been received. Then, the block points correctly to the last block in the blockchain. The stored data in any of the blocks cannot be altered because it will cause invalidation of all the data stored in the previous blocks of the block chain due to its hash function and this also leads to the breaking of consensus between the vehicles (nodes) associated with blockchain. Whereas, in the permissioned blockchain special case of a private blockchain, only authorized node have both write and read permission and public node only read the record but cannot able to add a new block in the chain. Auditing company and business intelligence company owners set up their own permissioned network, where nodes send the request to join the network after permissioned is granted, that worked in a decentralized blockchain manner. An alternative consensus algorithm named Proof of Stake (PoS) is used to add the new block in the network instead of PoW. In PoS, already exited nodes choose the leader among them that is responsible for creating the new block-based on their stake (trust availability). This reduces the computational time and cost concerning PoW based blockchain.

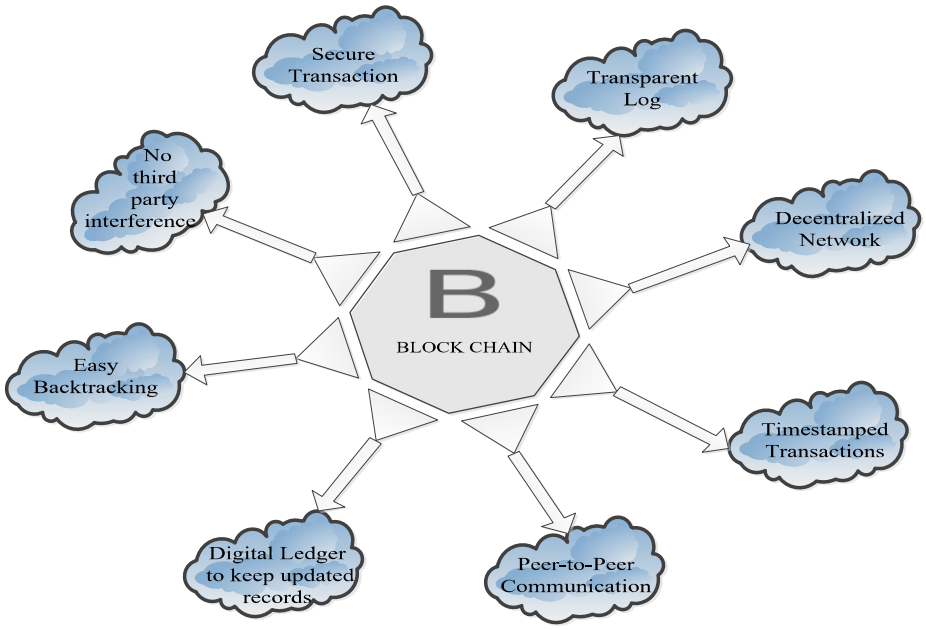



**Fig.5.4** Benefits of Blockchain Technology.

Each block has two parts, the header consists of a pointer (hash value) to the previous block and the latter is the body part that contains records of all the validated transactions, including users' information, time stamp, receipt, etc. as shown in Figure 5.5. This chain of blocks is formed by connecting the current block to the previous block by determining the hashed value of the current block using the hash value of the previous block. Here, all the vehicles (nodes) hold their own copy of their blockchain, and further to determine their current state, each transaction needs to be processed in the order of their appearance in the blockchain. The blocks present in the blockchain are partitioned into six sections as a hash function of the previous block in the blockchain, nonce, hash function associated with the current block, timestamp, Merkle root, and exchange data.

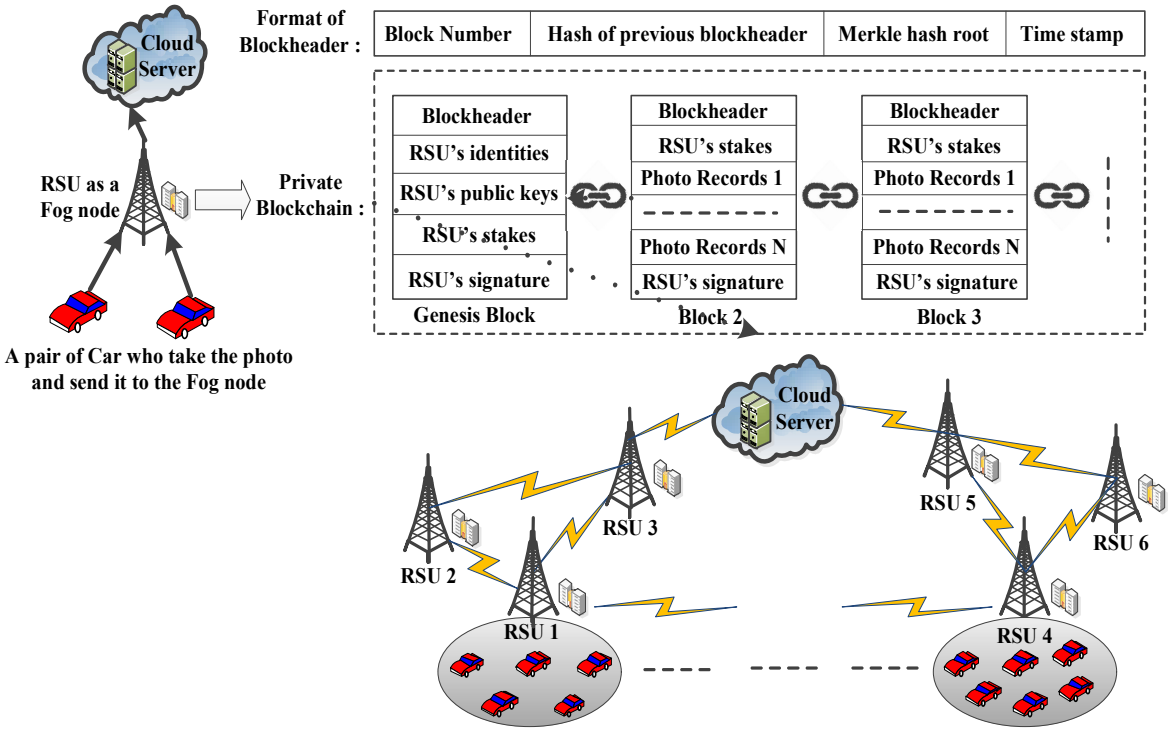



**Fig.5.5** Structure of Blockchain.

The blockchain is established on the pre-selected RSUs to share transaction records for audit that remove the authenticity of any intermediate trusted authority.

The RSUs (fog node), vehicle, cloud server construct a private block chain based on a consensus (PoS) mechanism. The smart contract (set of digital commitments) is an important factor in blockchain, where all the rules are predefined and executed when there is an event occurs, this rules cannot be modified once it is spread on the blockchain network. It ensures the transparent nature of the network, which encourages the vehicle to upload the picks of the SoI without worrying about their privacy leakage and finally economic benefit provided to the vehicle by the reception collection center. In this chapter, we proposed a security and privacy aware fog-cloud incentive based using a private blockchain approach to encourage the vehicles for uploading the picks of the site of interest.

## 5.3 Proposed Model

This section describes the privacy and security aware proposed model in IoV. We present a novel model for vehicle's privacy and securing the transferred data using pseudonym exchange mechanism through blockchain technique. The primary concern of the proposed model is to maintain scalability in terms of more vehicles participate in the service of upload the captured information to RSUs by providing incentives to participating vehicles. Later on, these rewards redeem on the RSU's as petrol pump for refueling.

On the other hand, providing static infrastructure all-over the roads to capture all the necessary information for every instant of time would cost the administration to an extreme. Instead of static infrastructure, we maintain mobile sensors to timely generate the necessary data to the cloud and save it for future purposes without any interference from outsiders or attackers. The vehicles (nodes) may be malicious and upload the wrong information to fog nodes so that, revocation authority identified those vehicles and put in a blacklist or revoke them. The privacy of vehicles and transaction of deposits (incentives) must not be leaked.

To counter the security and privacy problem, permissioned blockchain technique is used with PoS consensus mechanism. For system setup, several parameters are used and the initializations are discussed in the below subsections.

### 5.3.1 Preliminaries of System Initialization

Each vehicle conveys a bunch of pseudonyms imposed at the time of registration by DMV. To revoke a vehicle in IoV, encryption of a secret key is performed and this key is stored in RAs. Here, secret keys consist of the symmetric key which is used mainly for the generation of pseudonym denoted as $\mathcal{K}_{sk}$ and the individual secret key associated with each vehicle is denoted as $\mathcal{K}_{obu}$. For storing such keys in the RAs, an encryption algorithm known as the Elgamal encryption technique is used.

This technique is far better than Elliptic Curve Cryptography (ECC). Let us consider $\mathcal{G}$ as a cyclic group with prime order as $q$. A generator $\mathrm{G}$ is used to generate $\mathcal{G}$. At the time of registration of Vehicle the DMV, select any random number as a private key which is denoted as $k \in \mathcal{Z}^*$ and determine the public key using the mathematical expression $P\mathcal{K}^+ = k\mathrm{G}$. DMV holds the responsibility of distributing the shares of the secret keys to the RAs by using a secret share scheme based on a threshold. Here, $k$ is divided into $\ell$ equal parts and $\ell$ denotes the number of RAs so that each RA can hold a share of secret keys say $k_i$ where $k_i \in \{k_1, k_2, k_3 \dots \dots . k_\ell\}$ later, we can conclude that any existing secret sharing mechanism can be employed in such a process.

### 5.3.2 Tamper Resistant Hardware (TRH) Initialization

The installation and initialization of tamper resistant hardware devices in a vehicle are done at DMV. So, for this purpose, the owner of the vehicles needs to personally visit the DMV and the credential of the vehicles is confirmed. Then DMV initialized the TRH in the vehicle by saving several system parameters associated with the TRH. The parameters include $\{\mathcal{G}, q, \mathrm{G}, P\mathcal{K}^+, \mathcal{C}_{init}, \upsilon_{inc}\}$ where $\mathcal{C}_{init}$ denotes the secret initial counter of vehicles used in the generation of pseudonym and $\upsilon_{inc}$ denotes the factor to increment pseudonym. Also, DMV preloads vehicles TRH including secret keys such as $\mathcal{K}_{sk}$ and $\mathcal{K}_{obu}$.

### 5.3.3 Generation of Pseudonym

DMV is responsible for generating $\mathcal{n}$ number of vehicle pseudonym at the time of registration by considering the secret counter $\mathcal{C}_{init}$ of the vehicle and increment the counter by using the pseudonym incrementing factor $\upsilon_{inc}$. It is important to note that pseudonym is allowed to trace secretly to facilitate revocation whenever necessary by the RAs. TRH is a place for storing these pseudonyms and later used it for conditional privacy preserving communication process. The mathematical expression for generating pseudonyms is defined as follows:

$$\wp seu_{\mathcal{X}}^{i} = \{(\mathcal{E} \oplus V_{ID})_{\mathrm{K}_{obu}} \left|\left|(\mathcal{E})_{\mathrm{K}_{sk}}\right|\right| n_i\}_{\mathrm{K}_{DMV}} \tag{5.1}$$

Where $\mathcal{E} = \mathcal{C}_{init} + n_i \upsilon_{inc}$ and $n_i$ denotes the current count of the pseudonym that has been generated. $V_{ID}$ denotes the vehicle identification number. DMV records these pseudonyms in a database and index it through the value $\mathcal{n}$. All these pseudonyms and anonymous certificates are stored in TRH of the vehicles and distributed all these data to RAs too. These anonymous certificates are used mainly for exchange of pseudonym during the communication process. For the revocation process, the encryption of $\mathrm{K}_{obu}$ and $\mathrm{K}_{sk}$ is done by TRH and dispatch to the RAs. Here, in revocation process RAs play the role of trapdoor. The encryption of the previous keys with public master key based on ElGamal encryption technique is defined mathematically as follows:

$$C1 = r\mathrm{G} \text{ and } C2 = (\mathrm{K}_{obu}||\mathrm{K}_{sk}) \oplus H(rP\mathrm{K}^{+}) \tag{5.2}$$

Where $r$ denotes the random number generated only once (nonce) by TRH. The encrypted information, including $\{C1, C2\}$ is sent to RAs from TRH. On the other hand, decryption of $\mathrm{K}_{obu}$ and $\mathrm{K}_{sk}$ keys can also be carried out based on their warrant and construct $\mathcal{k}$ from separate $\mathcal{k}_i$ by cooperating. The main purposed for storing the encrypted keys in the database is for two reasons as in case of privacy any conflict; RAs used the keys for vehicle revocation. For each vehicle, the database is maintained by DMV, and the credentials of

the vehicles which includes $\{V_{ID}, C_{init}, \upsilon_{inc}\}$ are save.

### 5.3.4 Identity Exchange Using the Blockchain Technique

The identity related to the vehicles is the most important data that needs privacy preserving. The concept of multiple pseudonyms does not guarantee the enhancement of privacy as the pseudonym can be traced and relate to the sender. Hence, a new model for privacy preserving using the blockchain in identity (pseudonym) exchange mechanism has been proposed in this chapter. Each vehicle has its block to store the identity exchange record. The data are recorded in the blocks in an automatic and standardized manner so that if there is no trust between people, at least the user should have the option to believe that the code and system have been set up effectively and will work respectively.

The privacy of vehicles maintained by the pseudonym vehicles, that can be cancelled out whenever necessary. Based on the concept of DSRC, every vehicle in IoV is directed to broadcast the information to its nearby vehicle. This information includes current position, current speed, direction, etc. At a point when a vehicle needs to exchange pseudonyms with another vehicle by preserving its privacy, a beacon message is raised. An intent flag has also been included in the message to alert the vehicle for pseudonym exchange. In the meantime, all the nearby vehicles have a choice for exchanging the pseudonyms after receiving the beacon message. The beacon message is represented as

$$\mathcal{M}_{bea} = (B_{\boldsymbol{info}} || sec.primitives || intent)$$

Where $B_{\boldsymbol{info}}$ denotes the information, including position, acceleration, speed, heading, steering wheel angle, brake status etc. and, $sec.primitives$ denotes the parameters such as integrity, authentication, etc. To avoid a malicious attack of the exchange pseudonym, the process of exchanging the pseudonym should be anonymous. Since the knowledge of exchanging pseudonym provides probabilistic and statistical facility to the attackers. It is also important to note that, the validity of pseudonyms is checked before exchanging through the pseudonym revocation list. Meanwhile, the report for exchanging is sent to any

of the available RAs anonymously. And if the vehicle is favorable for exchanging the pseudonym, then RAs exchange the report. Further, it is noted that the benefit for revocation has been shared to all the RAs instead of sharing to a single entity.

The RSUs (fog node) maintains the private blockchain by collecting the real-time information, authentication of vehicles, data integrity, and finally upload the data to cloud server. Vehicle-vehicle identity exchange could be done on the ledger through smart contracts by employing the blockchain-verified identity.

A detailed overview of the smart contract is presented in algorithm 5.1. The $Init$ () function initialize the registration process of the vehicle obtain from DMV, vehicle $vI$ gets its certificate $cer_v$, which is used to identify itself with identity $ID_v$ and licence plate number $lnum_v$. Vehicle $v$ joins the blockchain network with identity $ID_v$ and able to gets its public and private keys $(pb_v, pv_v)$ and its wallet address $wa_v$ .

The vehicle $v$ execute the system initialization and upload its information $ID_v, lnum_v, pb_v, pv_v, cer_v, wa_v$ to nearest RSUs, where each information is stored into the memory block. To ensure the vehicle authenticity and their integrity of data, asymmetric encryption is used by RSUs signature in the blockchain as follow:

$$D_{pb_v}\left(Sig_{pv_v}(H(I))\right) = H(I) \tag{5.3}$$

Where $Sig_{pv_v}$ is the digital signature by sender's private key to the transferred information $I$, $H(I)$ is the hash digest of $I$ and $D_{pb_v}$ is the decode function of the information using sender public key.

The $create()$ function is used to implement new smart contract between the RSUs and vehicle $v$ on the agreement of the contract items through signed by their private keys. This smart contract is accessed by all the vehicles and RSUs deployed in the network after successfully verification of consensus mechanism. Each smart contract is responsible for maintain records such as state variables, account address of sender $(ac_v)$, account address of

RSUs $(ac_r)$ corresponding payment $\pi_v$ , timestamp $T_{stamp}$ and transaction time $T_{trans}$. In consensus (PoS) mechanism, where number of records in each RSUs treated as their respective stake or trust. For initial stake distribution, the Genesis block of the blockchain has RSUs identifies, public and stakes $(\{ID_r\}_{r=1}^{R}, \{pb_r\}_{r=1}^{R}, \{st_r\}_{r=1}^{R})$ respectively. Initially, genesis block is empty signed by Cloud server. After, leader is selected to generate new block among the RSUs using their probability of the previous block's stake. The newly created block has block header, block number, time stamp and Merkel hash root from the previous Merkle root hash root tree generated from previous records. Further, RSUs adds this newly block in the network by updating the stake value and records.

**Algorithm 5.1** Smart Contract between RSUs and Vehicle

1. ***Init*** ( ):
2. Input: $v, ID_v, lnum_v$
3. $\{cer_v, pb_v, pv_v, wa_v\} \leftarrow register(ID_v, lnum_v)$
4. ***Create***( ):
5. Input: $\mathcal{M}_{bea}, ac_v, ac_r, \pi_v, T_{stamp}, T_{trans}$
6. verify **(**$\mathcal{M}_{bea}, ac_v$**)**, verify **(**$ac_r \geq \pi_v$**)**
7. ***Invoke*** ( ):
8. **Input:** $SIO_v$
9. verify ($t \geq T_{trans}$)
10. send(v**,** $ac_v + \pi_v$ **)**

The $invoke$ ( ) function executed after the consensus and performed the smart contract between RSUs and vehicle if the $t \geq T_{trans}$ and perform the information (images of SoI ($SIO_v$)) transfer and incentive settlement. Further, the system automatically updates the ledger of the blockchains, state variables, and transfers the information to the cloud server. In this way, the proposed model is beneficial for the scalability in the IoV network that can keep up with a large number of vehicles. Unlike, PoW based public blockchains; the

proposed consensus (PoS) mechanism-based blockchain technology is carried out into small number of preselected RSUs and turn out to be reduction in both transaction latency and cost. Also, the total time to create a new block is stable regardless of the network size that ensures the anonymity of the vehicles which is maintained by the authorized RSUs.

### 5.3.5 Communication through Assisted Fog and Cloud

The sensor camera installed in a vehicle is intended to capture the full view of the sites (omnidirectional) known as the full view model. The working of these cameras is based on the density of the site where only specific vehicles were allowed to capture images in dense sites and in case of sparse sites most of the vehicles are allowed to take images to cover up the maximum area of the sites of interest. So, we assume that in case of the congested street there will be enough vehicles on the road to participate in the service. But, all the vehicles available on the busy road were not allowed to participate in the service because there will be wireless traffic due to an excessive amount of information. Hence, selected and mobile cameras around the street and attached to the vehicles play a vital role in such a situation.

### 5.3.6 Reporting of the Events and Acknowledgment

To encourage the participants involved in the service for capturing images of certain events happening on the road, we developed a model for providing a reward to the participants who provide accurate information regarding the events. Confidentiality will be maintained in this rewarding process. The steps involved in this process are described separately in the below section.

#### 5.3.6.1 Pictorial Event Reporting

The images captured by the vehicle are collected and the software timestamps together it with GPS data obtained from the GPS module which includes pseudonym pick up from the pool and sign and finally send the message to the cloud. The proper format of the message can be represented as:

$$message_{vehicle \rightarrow cloud} = (cert_{anonymous} \parallel Event_{ID} \parallel timestamp \parallel loc_V \parallel loc_E \parallel Qua_E \parallel \left(\wp seu_X^i \parallel IMG\right)_{pri})_{pub} \quad (5.4)$$

Where $cert_{anonymous}$ denotes the DMV issued anonymous certificates of the vehicle. $Event_{ID}$ represents the identity of the event. The location associated with vehicles is denoted by $loc_V$ and for the location of the event is denoted as $loc_E$ . $Qua_E$ Is the quality of the report of an event. $\wp seu_X^i$ Indicates the vehicle's pseudonym and $IMG$ denote the images taken by the vehicle. $pri$ and $pub$ denote the private and public key which are responsible for the secure communication process.

### 5.3.6.2 Collection of Receipt

After confirming the authorization and the contents presented by the contributors, the validity of the $cert_{anonymous}$ is verified by the receipt issuer and also examines the pseudonym validity. Once the validity is approved the cloud produces a receipt of the vehicle which contains a receipt ID. This ID act as a coupon to claim the reward. The format of the receipt issued to the vehicle and to the Receipt collector is represented as follows:

$$receipt_{issuer \rightarrow vehicle} = (cert_{anonymous} \parallel (Event_{ID} \parallel recei \quad _{ID} \parallel timestamp \parallel \wp seu_X^i)_{pub})_{pri}$$

$$receipt_{issuer \rightarrow collector} = (cert_{anonymous} \parallel (Event_{ID} \parallel receipt_{ID} \parallel timestamp \parallel \wp seu_X^i)_{pub} \quad (5.5)$$

Where $receipt_{ID}$ denotes the receipt ID. The above receipt format is necessary to claim the reward. Finally, cloud signs the receipt and later sent it to the vehicle.

### 5.3.6.3 Acknowledge

After receiving the receipt, the vehicles need to acknowledge to the cloud. Only after a valid acknowledgement, the coupon can be redeemed. Using this acknowledgement, users are

allowed to use the same pseudonym in the process of reporting and collecting the reward. The mathematical representation of acknowledgement is

$$ACK_{vehicle \to cloud} = (cert_{anonymous}, (receipt_{ID} \parallel timestamp \parallel \wp seu_{\chi}^{i} \parallel h_{pri_{vehic}} \ (contents)_{pub})_{pri} \quad (5.6)$$

Additionally, the hash value has been calculated by using its individual secret key and included in the acknowledgement to avoid from any case of conflict.

## 5.4 Adaptive Neuro-Fuzzy Based Payment

The reward is given to those participating vehicles, only after analyzing their services. This can be done by the use of the Adaptive Neuro-Fuzzy Inference System (ANFIS). ANFIS works on basically Artificial Neural Network (ANN) and Takagi-Sugeno Fuzzy Inference System (FIS).

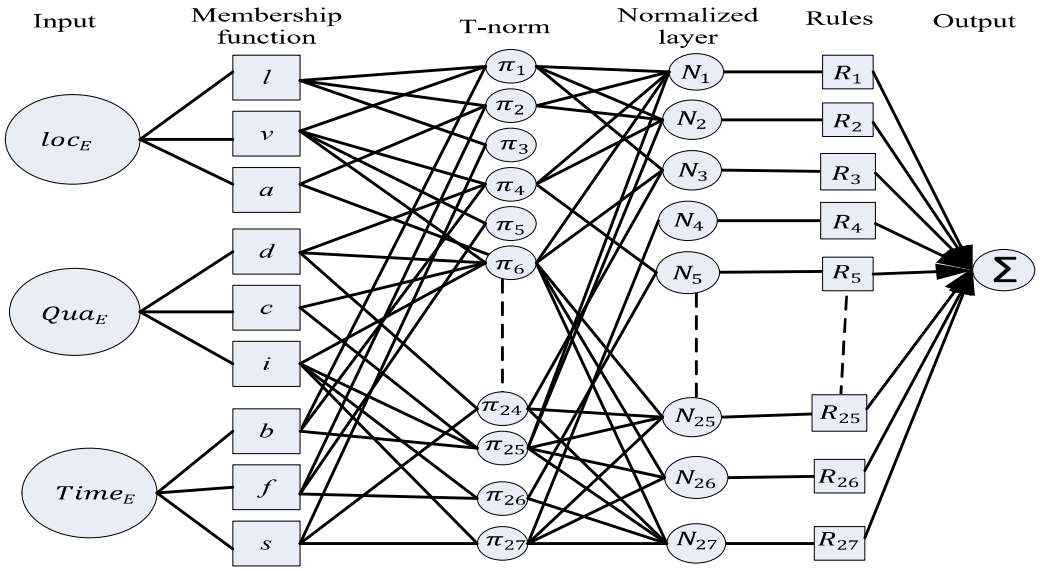



**Fig.5.6** Architecture of proposed ANFIS with three inputs and one output.

The ANN is used for weight adjustment of membership function to lower down the error rate inside the FIS according to feedback from the system. Location of event ($loc_E$),

timestamp of an event ($Time_E$) and Quality of report for an event ($Qua_E$) are feed as input to the proposed ANFIS for estimating the reward for a vehicle in the return of reporting an event shown in the Figure 5.6.

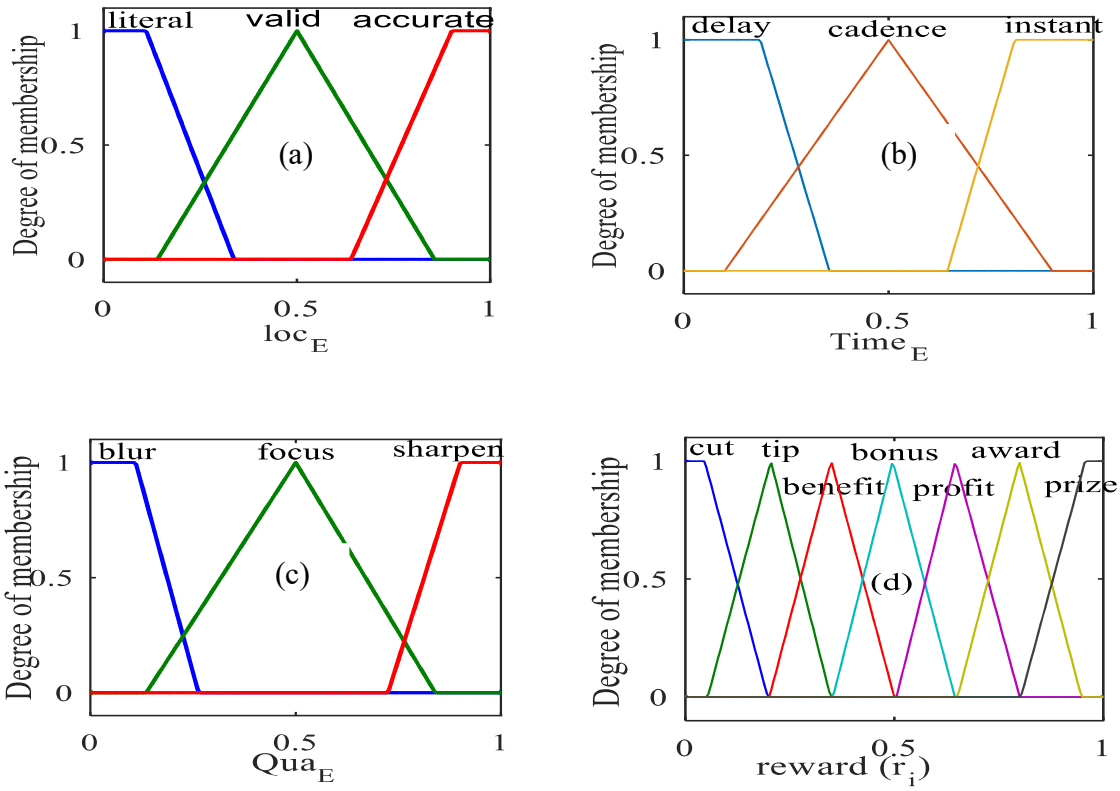



**Fig.5.7** Membership Function (a) $loc_E$ (b) $Time_E$ (c) $Qua_E$ (d) Reward($r_i$).

The linguistic variable for above parameters as follow: $loc_E(L)$ = {literal (l), valid (v), accurate (a)}, $Time_E(T)$ = {delay (d), cadence(c), instant (i)}, $Qua_E$ (Q) = {blur (b), focus (f), sharpen(s)} as shown in the Figure 5.7(a-c). The trapezoidal membership function is used for literal and accurate linguistic variables of the vehicle location, similarly, delay and instant linguistic variable of the reporting an event time and for blur and sharpen linguistic variable for the quality of the report an event uses trapezoidal membership function. The remaining linguistic variables valid, cadence, and clear for the $loc_E$ , $Time_E$ and $Qua_E$ uses triangular membership functions. The probability of the output (ANFIS) for the given input

parameters in terms of linguistic variable is a reward $r_i$ to the vehicle = {cut, tip, benefit, bonus, profit, award, and prize}. A similar membership function (triangular and trapezoidal) is used for the reward $r_{\#}^{i}$ as shown in Figure 5.7(d). Further, ANFIS consist of total $3^3 = 27$ rules pertain to three linguistic variables of each input parameter. These 27 rules ($r_{\#}^{i}$, (L, T, Q) are linear input parameter (antecedent) part and U is output parameter (consequent)) of If-Then for Takagi-Sugeno ANFIS are shown in Table 5.1.

**Table 5.1** If-Rules of ANFCA.

| Rule (#) | IF | | | THEN |
|---|---|---|---|---|
| | $loc_E$ | $Time_E$ | $Qua_E$ | $r_{\#}^{i} = (L) + t_{\#}(T) + q_{\#}(Q) + U_{\#}$ |
| 1. | *l* | *d* | *b* | *Cut* |
| 2. | *l* | *d* | *f* | *Cut* |
| 3. | *l* | *d* | *s* | *Tip* |
| 4. | *l* | *c* | *b* | *Cut* |
| 5. | *l* | *c* | *f* | *Tip* |
| 6. | *l* | *c* | *s* | *Benefit* |
| 7. | *l* | *i* | *b* | *Tip* |
| 8. | *l* | *i* | *f* | *Benefit* |
| 9. | *l* | *i* | *s* | *Benefit* |
| 10. | *v* | *d* | *b* | *Tip* |
| 11. | *v* | *d* | *f* | *Profit* |
| 12. | *v* | *d* | *s* | *Bonus* |
| 13. | *v* | *c* | *b* | *Profit* |
| 14. | *v* | *c* | *f* | *Benefit* |
| 15. | *v* | *c* | *s* | *Award* |
| 16. | *v* | *i* | *b* | *Bonus* |
| 17. | *v* | *i* | *f* | *Profit* |
| 18. | *v* | *i* | *s* | *Bonus* |
| 19. | *v* | *d* | *b* | *Benefit* |
| 20. | *a* | *d* | *f* | *Prize* |
| 21. | *a* | *d* | *s* | *Profit* |
| 22. | *a* | *c* | *b* | *Bonus* |
| 23. | *a* | *c* | *f* | *Bonus* |
| 24. | *a* | *c* | *s* | *Award* |
| 25. | *a* | *i* | *b* | *Award* |
| 26. | *a* | *i* | *f* | *Prize* |
| 27. | *a* | *i* | *s* | *Prize* |

The proposed ANFIS evaluate the output at fifth layer throughout processing the input parameter one by one each total of four layers. The working procedure of each layer as follow:

***(1) Fuzzy Layer-*** This layer is adaptive in nature due to weight of the membership function node (squared) is automatically tuned based on feedback. This layer uses triangular and trapezoidal membership function for plotting the membership function to evaluate the output $O_1$ as follow:

$$O_1(\gamma) = \mu_{\gamma_\tau}(\gamma)\ , \gamma\epsilon\{L, T, Q\}\ and\ \tau\epsilon\{l, v, a, d, c, i, b, f, s\} \tag{5.7}$$

Where, $\mu$ = {0, 1} define the degree of input according to membership function.

***(2) T-norm Layer-*** This layer non-adaptive in nature (circle with label π), it determines the firing strength of each rule associated with it as output ($O_2$) to the node. This can be done using minimize operator AND, which multiply each rule incident to the concerned node as follow:

$$O_2(\pi_\#) = \mu_{L_\tau}(L) * \mu_{T_\tau}(T) * \mu_{Q_\tau}(Q), \tag{5.8}$$

Where $\pi_\#$ represent the firing strength of each T-norm node.

***(3) Normalized Layer-*** Third layer is also non-adaptive type and mainly estimate the firing strength proportion of each rule coming from T-norm layer pertain to each node $N_\#$ labeled inside the circle. The output of normalized layer $O_2$ is calculated as follow:

$$O_3(N_\#) = \frac{\pi_\#}{\sum_\# \pi_\#} \tag{5.9}$$

***(4) Defuzzy Layer-*** This layer has the essence of adaptively tuned the firing strength of each rule pertain to square labeled node ($D_\#$). The output (consequent parameter) of fourth layer is the multiplication of individual firing strength and normalized firing strength of rule is calculated as follow:

$$O_4(R_\#) = N_\# * r_\# = \frac{\pi_\#}{\sum_\# \pi_\#} * (l_\#(L) + t_\#(T) + q_\#(Q) + U_\#) \quad (5.10)$$

***(5) Aggregated Output Layer-*** This non-adaptive layer estimated the final output of the ANFIS system treated as a performance evaluation layer. This can be done by summation of the signals coming to a single node represented with summation $\sum$ symbol inside single node as follow:

$$O_5 = \sum_\# N_\# * r_\# \quad (5.11)$$

The proposed ANFIS is used to calculate the reward in return of reporting an event by the vehicle represented as ANFPB in algorithm 2. The presented ANFPB work in two passes.

- ***Forward Pass-*** in this pass, input parameters are propagated from the first layer to the fourth layer and output of the defuuzy layer is note down. In this pass, all the antecedents' parameters are fixed but consequent parameters are updated. Further, the obtained output of the fourth layer is compared with the actual output ($A_o$) and Loss is estimated using a least square method as follow:

$$L\left(\mu_{\gamma_\tau}(\gamma), \mathrm{E}\right) = \frac{1}{2}\sum_{\gamma_\tau}(A_o(\gamma) - O_4(\gamma))^2 \quad (5.12)$$

- ***Backward Pass-*** In the meantime, Gradient descent method is used to minimize the error and the membership function is updated in the adaptive first layer node with the learning rate $\alpha\epsilon\{0,1\}$ as follow:

$$\nabla\mu_{,\gamma_\tau} L\left(\mu_{\gamma_\tau}(\gamma), \mathrm{E}\right) = \frac{\partial L\left(\ \gamma_\tau(\gamma)\right)}{\partial \mu_{\gamma_\tau}} \quad (5.13)$$

$$\mu_{\gamma_\tau}\left((\gamma), E+1\right) = \mu_{\gamma_\tau}(\gamma) + \alpha\nabla\mu_{,\gamma_\tau} L\left(\mu_{\gamma_\tau}(\gamma), \mathrm{E}\right) \quad (5.14)$$

At this time, consequents parameters are fixed. The complete backward and forward pass is known as one learning episode. The presented algorithm is run until convergence or a maximum number of episodes.

**Algorithm 5.2** Adaptive Neuro-Fuzzy Payment based on Blockchain (ANFPB)

1. **Begin**
2. **Input:** $\{L, T, Q\}$, $\alpha$ and Maximum number of episode $E_{max}$
3. **Output** {CH}
4. **For** E=1 to $E_{max}$.

   **// Forward pass**

   a. Degree of membership $O_1(\gamma)$ calculated using Eq. (7)

   b. Firing Strength of each rule $O_2(\pi_{\#})$ is calculated using Eq. (8)

   c. Normalized the firing strength of each rule using Eq. (9)

   d. Obtained the firing strength using Eq. (10)

   **//Backward pass**

   e. Estimated the error using Eq. (12)

   f. Update the weight $\mu_{\gamma_\tau}(\gamma)$ using Eq. (13) & Eq. (14)

5. Aggregated output is estimated using Eq. (11) at output layer.
6. **END**

## 5.4.1 Redeem Awards

The redeeming of awards is done by showing the coupon which has been collected from the cloud to Reward Collection Center (RCC) in cloud server as another physical entity by the users. The contents and the validity of the coupon are verified by RCC and further, the validity of the pseudonyms and the contribution is also verified by RCC. Besides this, RAs send the total amount of the reward to RCC and later provides the actual reward to the vehicle. Finally, all the reward transfer process is done through bitcoins.

## 5.4.2 Revocation System

An authorization letter is must be needed to carry out the revocation of a node. RAs are responsible for this process. The misconduct will be checked by the departments or expert

who includes law enforcement agencies, specialized expert, etc. The decision will be taken by these experts either to precede the issue a revocation or not. The first case is proceeding with the revocation; here RAs play the role of retrieving forensics data from the cloud. Then, according to the time interval as mention in the query, the data from the cloud is provided to the RAs. Later, RAs view the n values of the message to determine the pseudonym used and also search for the related pseudonym in Pseudonym Exchange History Table (PEHT) maintain by RAs to check whether the original owner used the pseudonym or it has been transacted with other users. Besides, PEHT is subject to make RAs know the next step. Based on the recent time the PEHT is searched, where RAs is responsible for constructing $\hbar$ from separate $\hbar_i$ by cooperating together which is related to the pseudonym and the cipher keys is decrypt in session leader. The mathematical expression for decrypt is represented as follows.

$$\wp seu_{\chi}^{i} = C2 \oplus H(\hbar C1)$$

$$= ((\mathcal{K}_{sk} \parallel \mathcal{K}_{obu}) \oplus H(r\, P\mathcal{K}^{+}) \oplus H(\hbar\, C1)$$

$$= (\mathcal{K}_{sk} \parallel \mathcal{K}_{obu}) \oplus H(rP\mathcal{K}^{+}) \oplus H(\hbar r\mathrm{G})$$

$$= (\mathcal{K}_{sk} \parallel \mathcal{K}_{obu}) \oplus H(r\hbar\mathrm{G}) \oplus H(\hbar r\mathrm{G})$$

$$= (\mathcal{K}_{sk} \parallel \mathcal{K}_{obu}) \tag{5.15}$$

Here, decryption of key $\mathcal{K}_{sk}$ and $\mathcal{K}_{obu}$ is performed by RAs and extract the vehicle identity based on the pseudonym.

## 5.5 Performance Evaluation

This section describes the qualitative performance evaluation of our proposed model subject to security and privacy preserving analysis, average transaction confirmation time, communication cost, anonymity, and attacking probability of the vehicle with respect to other state-of-art-models. We consider $5000 \times 5000\, m^2$city area that includes the

maximum number of 100 vehicles. We use NS-2 simulator to develop a simulation platform with varying speed of vehicle 20 to 80 km/h and the other simulation parameters is shown in Table 5.2.

**Table 5.2** Simulation parameters

| Parameter | Value |
|---|---|
| Number of RSU | [10] |
| Anonymity probability | [0, 0.95] |
| Attacking probability | [0, 0.95] |
| Beacon packet | 50 bytes |
| Beacon message interval | 1second |
| Data packet | 400 bytes |
| Acknowledgement packet | 60 bytes |
| OBU communication range | 300m |

## 5.5.1 Security Preserving Analysis

The main purpose of the proposed model is to preserve security and privacy. An attacker can observe the transaction or transmission of data happening between the vehicles as well as with the cloud. This attacker can analyze the obtained data, but it cannot analyses the pseudonym during the exchanging process because it is anonymous and encrypted before transfer. Hashing is performed using the secret key $\mathcal{K}_{sk}$ , as the sender holds this key the integrity of the data and non-repudiation is provided. This work only under the condition that the secret key cannot be compromised. Whereas if $\mathcal{K}_{obu}$ is compromised, then this alone cannot lead to hazards of the system as in this case only a part of the pseudonym can be obtained. But when we consider both the keys to be compromised, then the condition becomes more disastrous because attackers can easily use the pseudonym. For security purposes, the information about the events happening on the road is reported by the vehicles

on the cloud. Where the vehicle selects the $cert_{anonymous}$ and any $\wp seu_{\chi}^{i}$, later the message is signed and performs encryption using the public key of the cloud. It is worth to be noted that, unless if the vehicle did not compromise, the attacker can't interrupt the communication process. On the other hand, if both the keys (public and private) are compromised, then attackers can utilize the information associated with the events and even receive the award. In our proposed work such consequences are avoided and provide a secure environment.

## 5.5.2 Privacy Preserving Analysis

In case of privacy preserving, the vehicles report the events anonymously to the cloud so that the attackers are kept away from the original report generators. So, it is hard for the attackers to abuse the privacy of senders' messages. Especially, pseudonym exchange and anonymous reports make the attackers impossible to detect the original senders. Again, the vehicle ID present in the pseudonym act as a trap door in the revocation process. To measure the privacy of the event reports, we used entropy denoted by $\mathcal{S}$. The calculation of entropy depends on the anonymity set of the users denoted as $V$ (set of users encompasses the site of interest). Let's consider the chances of node $V_i$ to be as a witness among the sets of vehicles as $PV_i$ where a set of vehicles is denoted as $V = \{V_1, V_2 \dots \dots, V_i \dots\}$. And the entropy of node $V_i$ is defined mathematically as $\mathcal{S} = -\sum_{i=1}^{|V|} PV_i \times lo\ _2 PV_i$. Under normal distribution, the probable outcomes may be $|V|$ and the chance of each outcome is $1/|V|$. Since in this distribution every vehicle has equally likely changes in pseudonym exchange so maximum entropy can be achieved and the mathematical expression is represented as $S(max) = -\sum_{i=1}^{|V|} PV_i \times log_2 PV_i = lo\ _2 PV_i$. it is also important to know that normal entropy and maximum entropy are equal. We can further say that the entropy value does not depend only on the anonymity set; it also depends on the individual probability. In this situation, the more the items in anonymity set, the higher the entropy value. However, we consider variable anonymity sets based on its location and density of the traffic. Similarly, in the case of the rewarding process privacy preserving of the users is also maintained. This is

done by providing pseudo-identity at the reporting time. The pseudonym involved in such a case is selected by the users from the pool of its pseudonym.

Lastly, we can say that without compromising with the security parameters of the users it is hard for the attackers to access the information and remove the reward.

**Table 5.3** Comparative analysis of existing and proposed model based on several parameters.

| Model | $UA_U$ | $UA_n$ | $I_n$ | $UC_o$ | $P_t$ | $P_p$ | $ID_l$ | $R_w$ | $LC_o$ | $ID_d$ |
|---|---|---|---|---|---|---|---|---|---|---|
| J.S. Park et.al. [242] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ |
| S.B. Lee et. al.[243] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ |
| F. Li et. al.[244] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ |
| F.K. Tseng[245] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ | ✓ |
| Q. Li. et. al.[246] | ✗ | ✗ | ✗ | ✗ | ✓ | | ✓ | ✗ | | ✓ |
| J. M. F. et. al. [247] | ✗ | ✗ | ✗ | ✗ | ✓ | ✗ | | ✗ | ✗ | |
| Proposed Model | ✓ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |

## 5.5.3 Comparison of Proposed and Existing Schemes

The performance of our proposed work is evaluated based on certain parameters by comparing with the existing schemes. Even though the parameters used in existing and our proposed work are not comparable, we can still compare the privacy and security level provided in our posed work and existing work. Besides, the reward winning process can also be compared.

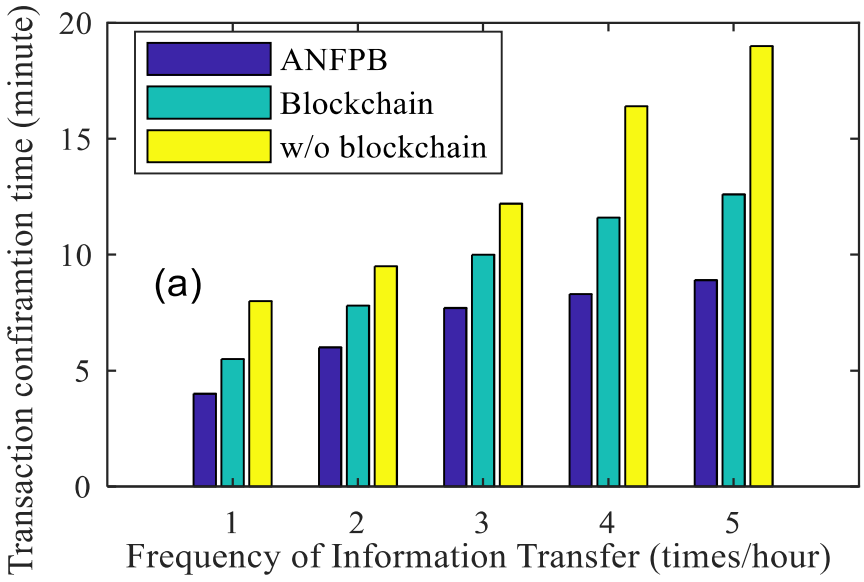
Table 5.3 represents the comparative analysis of existing schemes and the proposed model. In some of the existing schemes, the privacy of real identity is not maintained properly and this needs to be preserved for a secure life. After analyzing these existing methods, we can

determine that our proposed model is highly secure and also encourage the users to participate in operating the services successfully by providing privacy preserving of their real identity.

#### 5.5.3.1 Performance Analysis on PoS based Blockchain

The performance analysis of the proposed model ANFPB is done in terms of transaction confirmation time and transaction speed under the different frequency of information transfer with the traditional blockcahin model and without blockchain model. A number of information (images of SoI) transferred and their corresponding incentive is done in one hour referred to as transaction speed. Whereas, average total transaction confirmation time is referred to a number of consensus mechanisms finished for transactions for vehicles. For this purpose, we set the number of vehicles 40 for 240 minutes.

Similar to bitcoin, the traditional blockchain (PoW) model using cloud network, the transaction confirmation time is set to 60 minutes whereas in our proposed ANFPB blockchain (PoS) model using fog node is set to be 15 minutes. The pre-selected RSUs in our proposed model are set to be 10. The frequency of information and incentive transfer in our hour takes from the set value {1, 2, 3, 4, 5}.



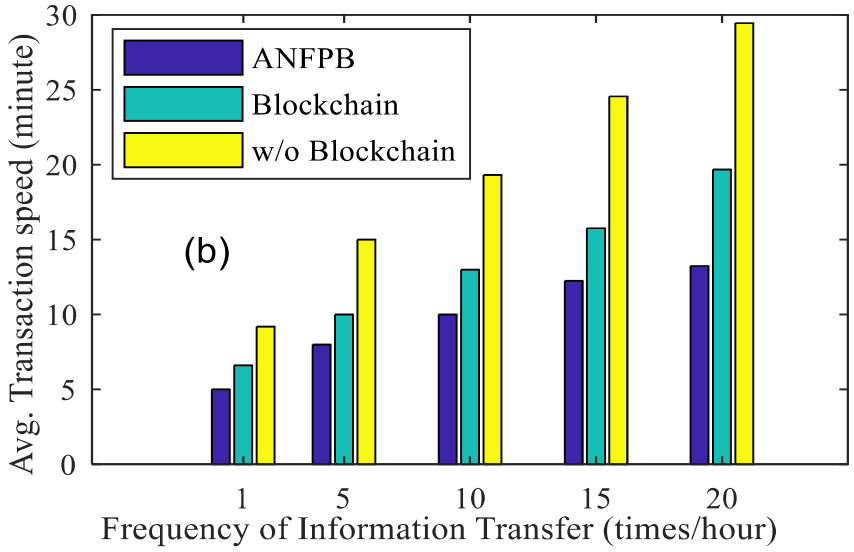



**Fig.5.8** Performance analysis: (a) Transaction confirmation time (b) Transaction speed.

Figure 5.8 (a) illustrate that as the frequency of information transferred and corresponding incentive are increases the total transaction confirmation time (average consensus mechanism per hour) increases sharply in blockchain (PoW) model than proposed model ANFPB blockchain (PoS) model. This is due to the fact that our proposed model carries out consensus process done by only preselected RSUs for information and incentive transfer than consensus process is done by all the RSUs in each vehicle of the blockchain (PoW) model.

Whereas Figure 5.8 (b) shows that average transaction speed (number of incentive transferred per hour) for one vehicle of the traditional blockchain approach is lower than the proposed blockchain model. This can be attributed to the adding of the fog layer to the cloud computing network, which increases the transaction speed and reduces the latency in credit the incentive to the respective vehicle in return for uploaded images of SoI. Thus, it is proved from the results, the proposed model supports fast transaction confirmation time and speed without much delay and it stabilizes on the increasing frequency of information transfer in fog-cloud based IoV network.

### 5.5.3.2 Computational Cost over Number of Vehicles

Figure 5.9 illustrates the computational cost (running time) on the RSUs to authenticate the registered vehicle. It is evident from the results as the number of vehicles increases the computational cost (second) in our proposed model is not increases sharply whereas the traditional blockchain model based on PoW increases sharply and there is the sharp increase in without blockchain model and not able to converged regardless of the number of vehicles.

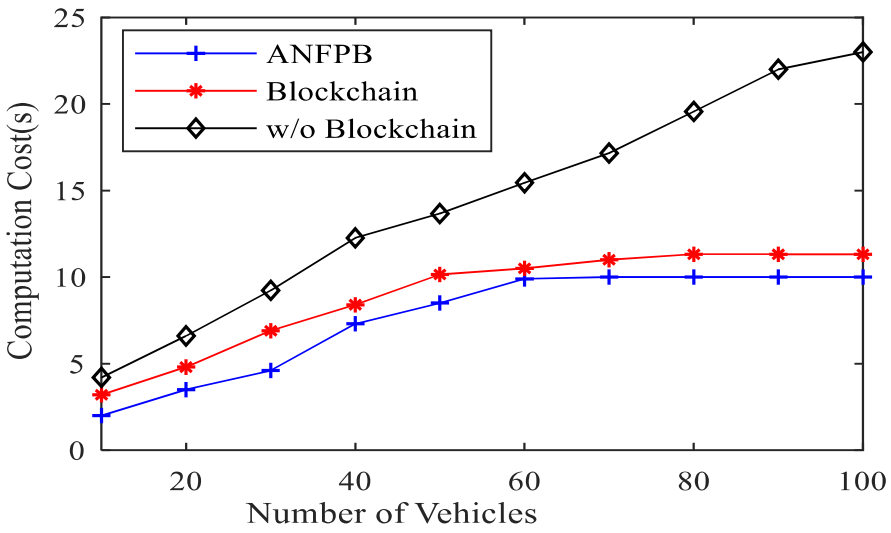
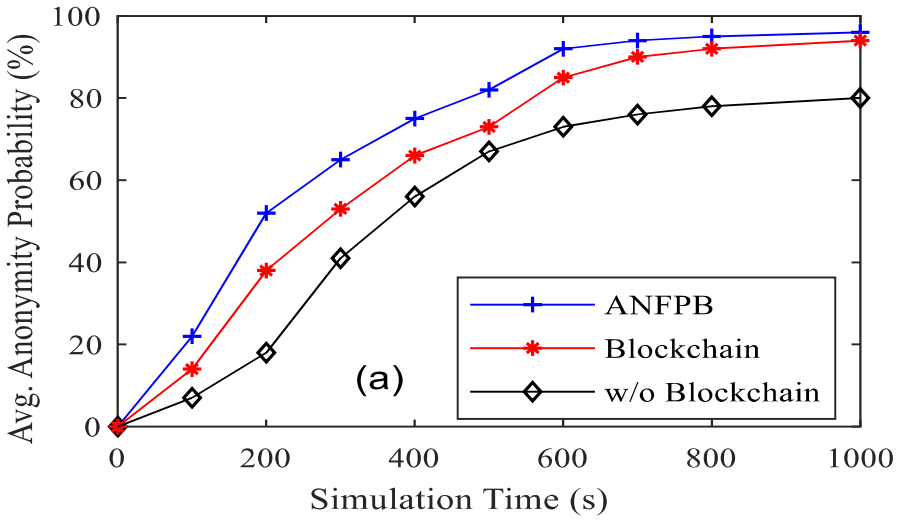



**Fig.5.9** Computation Cost(s) for vehicle authentication.

This can be attributed to the reason that the proposed model can efficiently authenticate the vehicles with fewer pairing on preselected RSUs, it does not require searching for the vehicles all over the fog-cloud based IoV network, accordingly running time is less than state-of-art algorithms. It is also worth noting down further increases in the vehicle over 60, the communication cost of the proposed model begins to stabilize. This is due to the fact proposed scheme efficiently reduce the latency of computing to generate, receive, transmit and a large amount of information in the proper way using blockchain with pseudonym mechanism.

#### 5.5.3.3 Anonymity and being Attack Probability by the Attackers over Simulation Time

For this purpose, we choose the number of vehicles in the fog-cloud based IoV network is 50. Figure 5.10 (a) compares the average probability of the vehicle's anonymity over increasing simulation time for the proposed model and state-of-art-models. It can be seen from the result, at the beginning of the simulation run, the anonymity of the vehicles is increasing sharply as the running time of the model increases in all of the models, but after 600 seconds the growth rate in the anonymity of the vehicles tend to stable. This is due to the fact, initially, more vehicles need to be anonymous by swapping pseudonyms, and after that, almost all vehicles have an anonymous identity then it tends to stabilize.




Whereas Figure 5.10 (b) shows the probability of being attack by outsider attackers for eavesdropping on the transferred confidential information or incentives given by RSUs in exchange for the images of SoI for the proposed model and state-of-art-models. From the above results of Figure 5.10 (a) assert that as the anonymity of the vehicles is increases, the probability of being attack by the attacker is gradually decreased. It can also be seen from the results, initially, the attack probability is 100% after that the simulation time ingresses as the probability of being attack is almost zero within 600 and 800 seconds for the proposed

ANFPB model and traditional blockchain with PoW model. Whereas worst performance is shown by without blockchain model, due to the fact our proposed model provides better pseudonym exchange mechanism with blockchain on preselected RSUs.

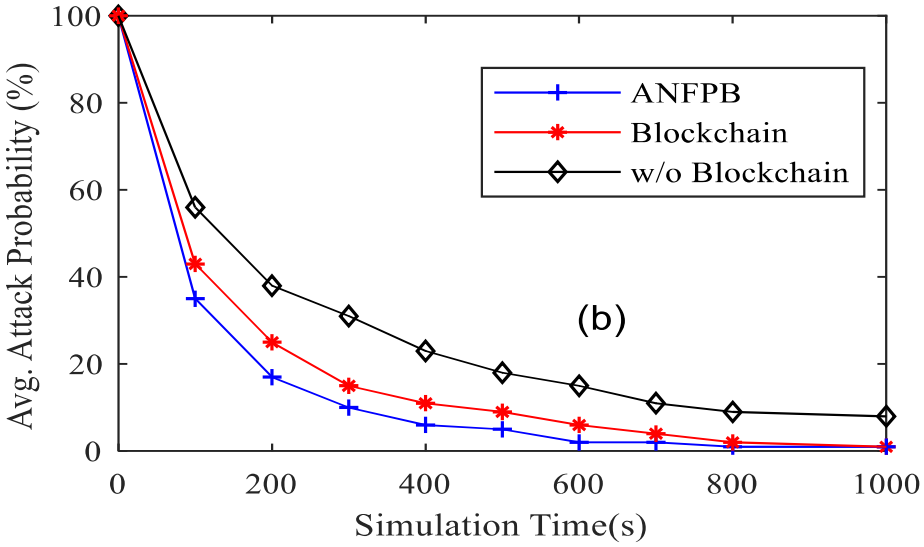



**Fig.5.10** Average probability over simulation time: (a) Anonymity (b) Attack.

#### 5.5.3.4 Anonymity and being Attack Probability of the Attackers over Vehicles

Figure 5.11 (a) shows the comparison of the average probability of vehicles anonymity overgrowth of vehicles in the simulation area of the fog-cloud based IoV network. It can be seen from the anonymity of the results of the vehicles shows an upward trend with respect to increasing in the vehicles up to 70, thereafter change in the probability of anonymity is negligible. This can be attributed as initially exchange in the pseudonym higher when the vehicle density is low and thereafter model reaches its optimal value and no longer fluctuation in anonymity probability of vehicle.

Whereas Figure 5.11 (b) shows the corresponding probability of being attacked by the outsider over increased vehicle density of proposed model and state-of-art-models. It is evident from Figure 5.11 (b), when the number of the vehicle is less than 20 the probability

of being attacked is above 80%, as the number of vehicles increases and the attack probability tends to decreases for all of the state-of-art-algorithms.

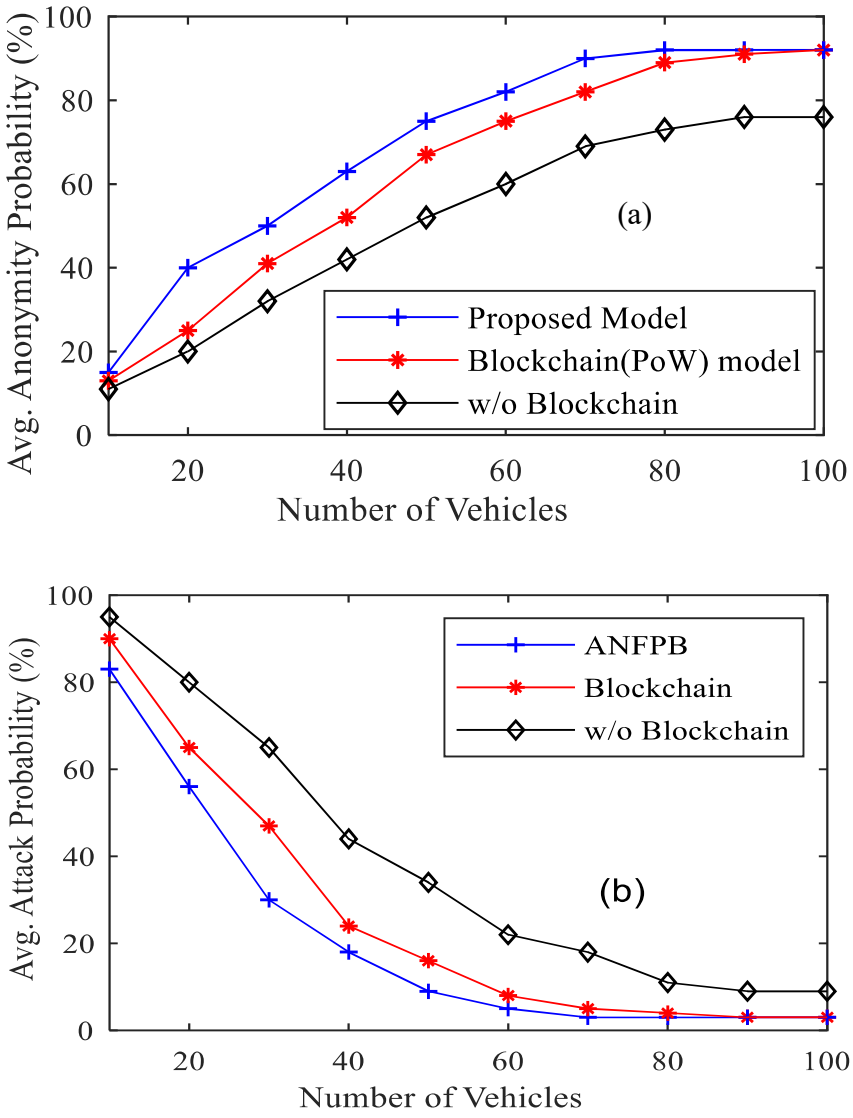



**Fig.5.11** Average probability over vehicle density: (a) Anonymity (b) Attack.

It is worth noting that for our proposed model the probability of being attacked by the outsider attacker is quickly stabilized to almost zero with only 70 vehicles with respect to other state-of-art-models. This is due to the fact fog layer assist in changing the pseudonym

with lower latency and accordingly, RSUs generate reports quickly using the blockchain approach. Therefore our proposed ANFPB model provides better anonymity and privacy with respect to vehicles density than other state-of-art-algorithms.

#### 5.5.3.5 Comparison of Reward over Different Incentive Algorithms

A comparison of reward over different type of an event with respect to state-of-art-algorithms shown in Figure 5.12, such as events are (i) Indifferent refers to the broken pavement (ii) Sensitive refers to the collision between one or more vehicles, catching fire on some vehicles (iii) Moderate refers to traffic congestion on the road, weather report. It is observed from the result that the value of reward of the proposed algorithm ANFPB is higher compared to other state-of-art algorithms.

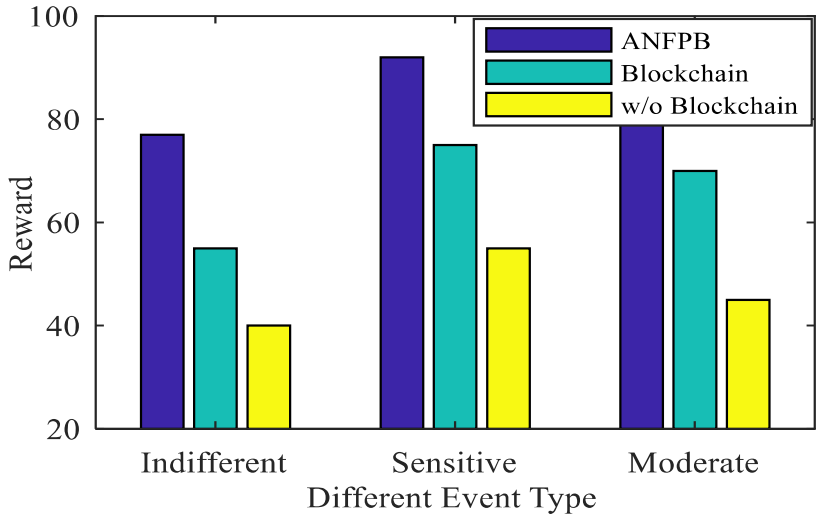



**Fig.5.12** Reward over different type of event report.

This is due to the fact proposed algorithm uses neuro-fuzzy ANFIS for the evaluation of reward based on event reporting within the timeline, location, and quality. Whereas blockchain based algorithm have not any learning approach to evaluating the reward. It is also a worthy point to note down that for the sensitive event the reporting must be within 10-15 minutes or live telecast of fire, causality or Collision preferred. In turn, proper action is taken by the concerned authority to save the life of involved persons. As a result, this type of

reporting causes more reward as compared to indifferent and moderate types. It is also seen from the result without the blockchain approach shows the worst performance in the evaluation of reward because it randomly put the reward value to any vehicles.

#### 5.5.3.6 Comparison of Reward over Event Duration

A comparison of reward value over event duration with respect to state-of-art-algorithms as shown in Figure 5.13, as the time duration increases the consequently larger number of reports are generated and uploaded to the fog layer by the vehicles. It is evident from the result the as the time duration increases consequently the reward value is also increased up to 90Rs for the proposed algorithm and remains constant afterward. This is because as the time duration increases some of the reports (sensitive ones) have less impact if they are report delay, some of the event (road breakage) last longer than a day and as a result, the value of a reward is not increased further sharply.

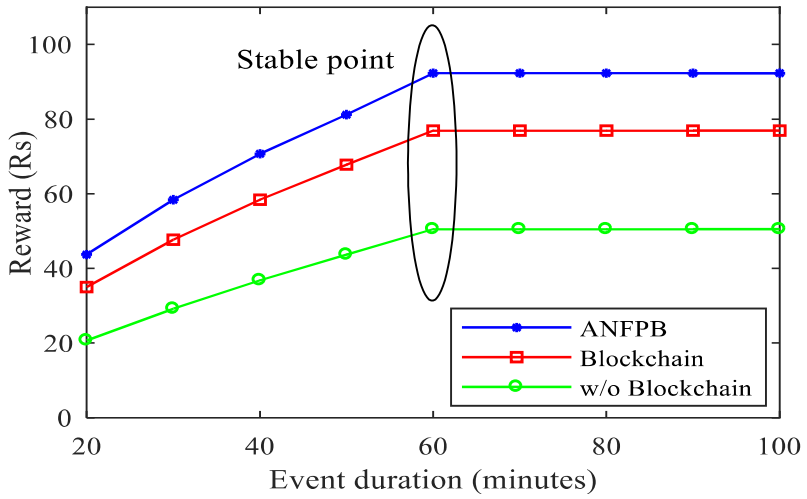



**Fig.5.13** Reward over event duration.

This can be attributed to the reason that reward value reaches up to the maximum limit. It can be also seen from the result the reward value of the traditional blockchain and w/o blockchain algorithm also increases but they are lagging behind 14% and 24% respectively from proposed ANFPB algorithms. This is due to the fact blockchain based algorithm

evaluates the reward value using a simple mathematical model and does not able to adapt the reward value according to changes in the location, timeline, and quality of the report sent by the vehicles. Whereas w/o blockchain shows the worst performance because of it evaluates the reward value without considering the period of the event reported.

## 5.6 Summary

In this chapter, a novel adaptive neuro-fuzzy based payment using blockchain scheme to preserve the privacy of vehicles in the process of information sharing and also encourage vehicles to participate in the information sharing with RSU in IoV network. A smart contract is also proposed to register the vehicles themselves using an identity exchange process to provide more secure privacy from any attackers to access the contents in midway. Meanwhile, we also introduced the rewarding of most active users in the IoV network to encourage the users to participate using the neuro-fuzzy technique algorithm ANFPB. The simulation results show that our proposed model ANFPB preserves the security and privacy of the users, and encourages the users to participate in the service that also helps to capture the correct evidence of any events happening on the road as compared to other state-of-art-algorithms. In the future, we would like to extend this work by advancing machine learning techniques with blockchain. And, also includes the compression of huge data in the cloud to preserving their security.

# Chapter 6

# Conclusion and Future work

Due to the continuous evolution of communication technologies, IoV attracts large number of leading commercial company as well as researchers. IoV has drawn a lot of attention among the researchers, scientists, and practitioners due to its wide range of applications in various fields. This thesis systematically studies the several security issues of IOV and proposes an efficient model on video streaming in urban vehicular environments. In addition, this thesis addresses the privacy issue of vehicles in 5G and beyond IoV Networks. This chapter outlines the main achievements of this thesis and points out the directions for future research.

The remaining part of the chapter is structured as follows: Section 6.1 contains the conclusion of the thesis. The future work is explained in section 6.2.

## 6.1 Conclusion

IOVs have become a promising technique due to its broad range of applications in several fields. IoV can deal with global information by allowing the devices located in a larger range (whole country) to communicate. IoV is based on the intelligent integration of vehicles, human, things and surrounding environments. Due to the accessibility of devices located at large range, it has more commercial interests in comparison to VANETs and also reduces traffic congestion. Hence, IoV is term as the platform for information exchange among the devices in the network in a direct or indirect manner. This implements a secure, safer, efficient, robust and greener environment transportation network. The detailed description of our contribution is listed below in the form of chapters.

The main aim of first chapter was to present a brief introduction as well as motivation for IOVs. The chapter discussed the introduction of IoV is given along with the applications, architecture, protocol stack, network model and challenging issues of IoV. It further

identified various issues and security requirements for IoV. In addition to this, research problems and research objectives are formulated. Additionally, a methodology has been discussed to accomplish these objectives. The concept of security and privacy is also discussed in brief. At last, the thesis outline and summary of the chapter is presented.

The second chapter discussed relevant, good quality detailed literature reviews on video streaming in urban vehicular environments: junction-aware multipath approach. Furthermore, we discuss the current work on location privacy-preserving (LP-preserving) in IOVs. Moreover, we discuss the methods with their advantage for efficient privacy-preserving. Then we identify different types of IoV architecture based on the interaction of various innovations in the IoV environment. We provide existing IoV architecture models, their different types of layers, and their functionality in a tabular form.

The chapter three has discussed the first objective of the thesis which is known as an efficient model on video streaming in urban vehicular environments considering different points at the junction area in order to avoid or minimize video packet error or drop. Further, some mathematical formulations have been adapted to estimate the suitability of a node for data packet delivery. An enhanced vehicle selection considering the different points in the junction area in order to minimize packet drop due to changes of vehicle direction in the junction area. We incorporate improved vehicle selection based on link quality calculation, considering the signal to interference plus noise ratio (SINR), in order not to select vehicles with high noise due to obstructing objects in the urban environment.

The chapter four has discussed the second objective of the thesis that designs an efficient lightweight location authentication scheme for VANET. We discuss that privacy as well as authentication is the most important part of VANETs since various attacks such as location tracking and identity revealing steal sensitive information to create considerable risk for human lives. The attacker changes confidential information such as speed, direction, path, location of vehicle owner, and exploits its privacy. The existing privacy-preserving schemes like pseudonym schemes, anonymous signing protocol, group signature, and authentication-

based schemes, mix zone and silent period, etc. are inefficient in terms of storage, privacy-preserving, and implementation. Furthermore, they impose high overhead and converges very slowly.

The chapter five has discussed the third objective of the thesis that designs an adaptive Neuro-Fuzzy based payment scheme using block chain to ensure privacy of vehicles in 5G and beyond IoV Networks. A smart contract is also proposed to register the vehicles themselves using an identity exchange process to provide more secure privacy from any attackers to access the contents in midway. Meanwhile, we also introduced the rewarding of most active users in the IoV network to encourage the users to participate using the Neuro-fuzzy technique algorithm known as ANFPB. The simulation results show that our proposed model ANFPB preserves the security and privacy of the users, and encourages the users to participate in the service that also helps to capture the correct evidence of any events happening on the road as compared to other state-of-art-algorithms.

## 6.2 Future Work

As we know, a considerable amount of research work has been carried out on security and privacy for IOV, but still, new research problems, as well as challenges, emerges with the development of IOV applications. Motivated by the research challenges discussed in the existing works as well as in this thesis, we identified a series of future works that are listed as follows.

In chapter three, we proposed an efficient model on video streaming in urban vehicular environments considering different points at the junction area in order to avoid or minimize video packet error or drop. Future research should focus on different kinds of roads including highway bridges and bent roads, considering their effects on video data packet forwarding to achieve quality video streaming in VANETs.

The chapter four designs an efficient lightweight location authentication scheme for VANETs. In the future, we can use more optimal and robust keys in ID-based cryptosystem

and pseudonym to improve privacy of vehicles. Moreover, we can incorporate an empirical vehicle tracker in VANETs.

In chapter five, in the future, we would like to extend this work by advancing machine learning techniques [48] with blockchain and, also includes the compression of huge data in the cloud to preserving their security.

# References


[1] J. Kang et al.,“Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol.8, no. 19, pp.2627-2637, 2017.

[2] Lopez, Héctor Jalil Desirena, Mario Siller, and Iván Huerta. "Internet of vehicles: Cloud and fog computing approaches." In 2017 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), vol. 11, pp. 211-216. IEEE, 2017.

[3] L. A. Maglaras et al., “Social Internet of vehicles for smart cities,” Journal of Sensor and Actuator Networks, vol. 5, no. 3, pp. 3-17, 2016.

[4] M. Chaqfeh, A. Lakas, and I. Jawhar, “A survey on data dissemination in vehicular ad hoc networks,” Vehicular Communication., vol. 1, no. 4, pp. 214–225, Oct. 2014.

[5] A. Al-Fuqaha, M.Guizani, M. Mohammadi, M. Aledhari, and M.Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE Communications Surveys &Tutorials Vol. 17, No. 4, pp.2347- 2376, 2015.

[6] Bonomi, Flavio, Rodolfo Milito, Jiang Zhu, and Sateesh Addepalli. "Fog computing and its role in the internet of things." In Proceedings of the first edition of the MCC workshop on Mobile cloud computing, pp. 13-16. 2012.

[7] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, “A comprehensive survey on vehicular ad hoc network,” J. Netw.Comput. Appl., vol. 37, pp. 380–392, Jan. 2014.

[8] Sherazi, Hafiz Husnain Raza, Zuhaib Ashfaq Khan, Razi Iqbal, Shahzad Rizwan, Muhammad Ali Imran, and Khalid Awan. "A heterogeneous IoV architecture for data forwarding in vehicle to infrastructure communication." Mobile Information Systems vol.5, pp. 1022-1035, Feb 2019.

[9] J. Cheng et al., "Routing in Internet of vehicles: a review," IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 5, pp. 2339-2352, October 2015.

[10] J. Guerrero-Ibanez, C. Flores-Cortes, and S. Zeadally, "Vehicular ad-hoc networks (VANETs): Architecture, protocols, and applications," in Next Generation Wireless Technologies: 4G and Beyond, N. Chilamkurti, S. Zeadally, and H. Chaouchi, Eds. London, U.K. vol.1, pp. 49-70, Springer, 2013.

[11] J. Raymond, "The Internet of Things: A study in hyper, reality, disruption and growth," U.S. Res. Published Raymond James Assoc., St. Petersburg, FL, USA, Tech. Rep. vol. 1 pp. 35-49, 2014.

[12] Matthew N. O. Sadiku, Mahamadou Tembely, and Sarhan M. Musa," Internet of Vehicles: An Introduction", International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X, Vol. 8, no.-1, pp. 11-13, Feb 2018.

[13] G. Dimitrakopoulos, "Intelligent transportation systems based on Internet-connected vehicles: Fundamental research areas and challenges," in Proc. 11th Int. Conf. ITS Telecommun., St. Petersburg, Russia, ,vol. 1, pp. 145–151, Aug. 2011.

[14] The White House, US "National Strategy for Trusted Identities in Cyberspace (NSTIC): Enhancing Online Choice, Efficiency, Security, and Privacy", 2011. Available: https://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[15] Transport Department, GOVT of NCT of Delhi, "Installation of GPS in buses and autos", Order No: Odr(2010)/75/8, 2010.

[16] European Commission, "Digital Signal Market Strategy", 2015. Available: http://ec.europa.eu/priorities/digital-single-market/.

[17] Uni. of Michigan, "Public opinion about self-driving vehicles in China, India, Japan, the U.S., the U.K., and Australia", UMTRI, pp. 122, 2014. Available: http://deepblue.lib.umich.edu/bitstream/handle/2027.42/06590/102996.pdf?sequence=1&isAllowed=y.

[18] Google. (2015). Open Automobile Alliance. [Online]. Available: http://www.openautoalliance.net/.

[19] Apple, “CarPlay”, 2014. Available: http://www.apple.com/ios/carplay/.

[20] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, “Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp.2377-2396, 2015.

[21] Contreras-Castillo, Juan, Sherali Zeadally, and Juan Antonio Guerrero Ibáñez. “Seven-layered model architecture for Internet of Vehicles." Journal of Information and Telecommunication 1, vol. 1, no. 1, pp. 4-22, 2017.

[22] Kaiwartya, Omprakash, Abdul Hanan Abdullah, Yue Cao, Ayman Altameem, Mukesh Prasad, Chin-Teng Lin, and Xiulei Liu. "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects." IEEE Access vol. 4, pp. 5356-5373, 2016.

[23] K. Zheng, Q. Zheng, P. Chatzimisios, W. Xiang, and Y. Zhou, “Heterogeneous Vehicular Networking: A Survey on Architecture, Challenges, and Solutions” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp.2377-2396, 2015.

[24] Yang, Fangchun, Shangguang Wang, Jinglin Li, Zhihan Liu, and Qibo Sun. "An overview of internet of vehicles." China communications, vol. 11, no. 10, pp. 1-15, 2014.

[25] Department of Transportation, US “Connected vehicle Research”, 2015. Available: http://www.its.dot.gov/research.htm.

[26] Tiwari, Priyanka, and Rajendra Singh Kushwah. "Traffic analysis for VANET using WAVE and WiMAX." In 2015 International Conference on Communication Networks (ICCN), vol. 1, pp. 343-346. IEEE, 2015.

[27] Bello, Oladayo, and Sherali Zeadally. "Intelligent device-to-device communication in the internet of things." IEEE Systems Journal, vol. 10, no. 3, pp. 1172-1182, 2014.

[28] Vermesan, Ovidiu, Peter Friess, Patrick Guillemin, Harald Sundmaeker, Markus Eisenhauer, Klaus Moessner, Franck Le Gall, and Philippe Cousin. "Internet of things strategic research and innovation agenda." In Internet of things: converging technologies for smart environments and integrated ecosystems, River Publishers, vol. 1, pp. 7-152, 2013.

[29] L. Armstrong, and W. Fisher, "IEEE Std 802.11P Wireless Access for Vehicular Environment", Project Report, Internet Task Force (IETF), 2010.Available: https://www.ietf.org/mailarchive/web/its/current/pdfqf992dHy9x.pdf.

[30] IEEE Working Group for Wireless Standard, "IEEE 802.11TM Wireless Local Area Networks", Available: http://www.ieee802.org/11/.

[31] IEEE 802.16 based standards, "WiMax Forum-Technology", Available: http://www.wimaxforum.org/.

[32] C. Cox, "An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications", 1st ed., John Wiley & Sons, UK, vol. 1, pp. 208-219, 2012.

[33] Wu, Weigang, Zhiwei Yang, and Keqin Li. "Internet of Vehicles and applications." In Internet of Things, Morgan Kaufmann, vol. 1 pp. 299-317., 2016.

[34] Hsu, Robert C-H., and Shangguang Wang. "Internet of vehicles–technologies and services." In First International Conference, IOV. 2014.

[35] Tan, Han-Shue, and Jihua Huang. "DGPS-based vehicle-to-vehicle cooperative collision warning: Engineering feasibility viewpoints." IEEE Transactions on Intelligent Transportation Systems, vol. 7, no. 4, pp. 415-428, 2006.

[36] Miller, Ronald, and Qingfeng Huang. "An adaptive peer-to-peer collision warning system." In Vehicular Technology Conference. IEEE 55th Vehicular Technology Conference. VTC Spring 2002 (Cat. No. 02CH37367), vol. 1, pp. 317-321. IEEE, 2002.

[37] Biswas, Subir, Raymond Tatchikou, and Francois Dion. "Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety." IEEE communications magazine vol. 44, no. 1, pp. 74-82, 2006.

[38] Reichardt, Dirk, Maurizio Miglietta, Lino Moretti, Peter Morsink, and Wolfgang Schulz. "CarTALK 2000: Safe and comfortable driving based upon inter-vehicle-communication." In Intelligent Vehicle Symposium, 2002. IEEE, vol. 2, pp. 545-550. IEEE, 2002.

[39] Yang, Xue, Leibo Liu, Nitin H. Vaidya, and Feng Zhao. "A vehicle-to-vehicle communication protocol for cooperative collision warning." In The First Annual

International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004., pp. 114-123. IEEE, 2004.

[40] Taleb, Tarik, Abderrahim Benslimane, and Khaled Ben Letaief. "Toward an effective risk-conscious and collaborative vehicular collision avoidance system." IEEE Transactions on Vehicular Technology 59, no. 3, pp. 1474-1486, 2010.

[41] Milanes, Vicente, Jorge Villagrá, Jorge Godoy, Javier Simó, Joshué Pérez, and Enrique Onieva. "An intelligent V2I-based traffic management system." IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 49-58, 2012.

[42] Maruoka, Tetuya, Yasuhiro Sato, Shinji Nakai, Tomotaka Wada, and Hiromi Okada. "An extended collision judgment algorithm for vehicular collision avoidance support system (VCASS) in advanced ITS." In 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5. IEEE, 2008.

[43] Chen, Po-Yu, Yi-Min Guo, and Wen-Tsuen Chen. "Fuel-saving navigation system in VANETs." In 2010 IEEE 72nd Vehicular Technology Conference-Fall, pp. 1-5. IEEE, 2010.

[44] Collins, Kevin, and Gabriel-Miro Muntean. "Route-based vehicular traffic management for wireless access in vehicular environments." In 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5. IEEE, 2008.

[45] Chim T, Yiu S, Hui L, Li V. "VSPN: VANET-based secure and privacy-preserving navigation". IEEE Trans Comp, vol. 2,no. 63, pp. 510-524, 2014.

[46] Leontiadis, Ilias, Gustavo Marfia, David Mack, Giovanni Pau, Cecilia Mascolo, and Mario Gerla. "On the effectiveness of an opportunistic traffic management system for vehicular networks." IEEE Transactions on Intelligent Transportation Systems,vol.12, no. 4, pp. 1537-1548, 2011.

[47] Verroios, Vasilis, Vasilis Efstathiou, and Alex Delis. "Reaching available public parking spaces in urban environments using ad hoc networking." In 2011 IEEE 12th International Conference on Mobile Data Management, vol. 1, pp. 141-151. IEEE, 2011.

[48] Lu, Rongxing, Xiaodong Lin, Haojin Zhu, and Xuemin Shen. "SPARK: A new VANET-based smart parking scheme for large parking lots." In IEEE INFOCOM 2009, pp. 1413-1421. IEEE, 2009.

[49] Hunt, P. B., D. I. Robertson, R. D. Bretherton, and M. Cr Royle. "The SCOOT on-line traffic signal optimisation technique." Traffic Engineering & Control, vol. 23, no. 4, 2018.

[50] Sims, Arthur G., and Kenneth W. Dobinson. "The Sydney coordinated adaptive traffic (SCAT) system philosophy and benefits." IEEE Transactions on vehicular technology, vol. 29, no. 2, pp. 130-137, 2019.

[51] Maslekar, Nitin, Mounir Boussedjra, Joseph Mouzna, and Houda Labiod. "VANET based adaptive traffic signal control." In 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring), pp. 1-5. IEEE, 2011.

[52] Gradinescu, Victor, Cristian Gorgorin, Raluca Diaconescu, Valentin Cristea, and Liviu Iftode. "Adaptive traffic lights using car-to-car communication." In 2007 IEEE 65th vehicular technology conference-VTC2007-Spring, pp. 21-25. IEEE, 2007.

[53] Prashanth, L. A., and Shalabh Bhatnagar. "Reinforcement learning with function approximation for traffic signal control." IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 2, pp. 412-421, 2010.

[54] Wunderlich, Richard, Cuibi Liu, Itamar Elhanany, and Tom Urbanik. "A novel signal-scheduling algorithm with quality-of-service provisioning for an isolated intersection." IEEE Transactions on Intelligent Transportation Systems, vol. 9, no. 3, pp. 536-547, 2018.

[55] Li, Chunxiao, and Shigeru Shimamoto. "An Open Traffic Light Control Model for Reducing Vehicles CO2 Emissions Based on ETC Vehicles." IEEE transactions on vehicular technology, vol. 61, no. 1, pp. 97-110, 2011.

[56] Cai, Chen, Yang Wang, and Glenn Geers. "Adaptive traffic signal control using vehicle-to-infrastructure communication: a technical note." In Proceedings of the Third International Workshop on Computational Transportation Science,vol. 1, no. 1, pp. 43-47. 2010.

[57] Priemer, Christian, and Bernhard Friedrich. "A decentralized adaptive traffic signal control using V2I communication data." In 2009 12th International IEEE Conference on Intelligent Transportation Systems, pp. 1-6. IEEE, 2009.

[58] Lin, Wei-Hua, and Chenghong Wang. "An enhanced 0-1 mixed-integer LP formulation for traffic signal control." IEEE Transactions on Intelligent transportation systems, vol. 5, no. 4, pp. 238-245, 2014.

[59] Qiao, Jian, Naiding Yang, and Jie Gao. "Two-stage fuzzy logic controller for signalized intersection." IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, vol.41, no. 1, pp. 178-184, 2010.

[60] Abdulhai, Baher, Rob Pringle, and Grigoris J. Karakoulas. "Reinforcement learning for true adaptive traffic signal control." Journal of Transportation Engineering 129, no. 3 , pp. 278-285, 2013.

[61] El-Tantawy, Samah, and Baher Abdulhai. "An agent-based learning towards decentralized and coordinated traffic signal control." In 13th International IEEE Conference on Intelligent Transportation Systems, pp. 665-670. IEEE, 2010.

[62] Milanes, Vicente, Jorge Villagrá, Jorge Godoy, Javier Simó, Joshué Pérez, and Enrique Onieva. "An intelligent V2I-based traffic management system." IEEE Transactions on Intelligent Transportation Systems, vol. 13, no. 1, pp. 49-58, 2011.

[63] Glaser, Sébastien, Benoit Vanholme, Saïd Mammar, Dominique Gruyer, and Lydie Nouveliere. "Maneuver-based trajectory planning for highly autonomous vehicles on real road with traffic and driver interaction." IEEE Transactions on intelligent transportation systems, vol. 11, no. 3, pp. 589-606, 2010.

[64] Milanés, Vicente, Joshué Pérez, Enrique Onieva, and Carlos González. "Controller for urban intersections based on wireless communications and fuzzy logic." IEEE Transactions on Intelligent Transportation Systems, vol. 11, no. 1, pp. 243-248 2019.

[65] Dresner, Kurt, and Peter Stone. "Multiagent traffic management: A reservation-based intersection control mechanism." In Autonomous Agents and Multiagent Systems, International Joint Conference on, vol. 3, pp. 530-537. IEEE Computer Society, 2014..

[66] Dresner, Kurt, and Peter Stone. "Multiagent traffic management: An improved intersection control mechanism." In Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems, vol. 1, no. 1, pp. 471-477. 2015.

[67] Gehring, Ottmar, and Hans Fritz. "Practical results of a longitudinal control concept for truck platooning with vehicle to vehicle communication." In Proceedings of Conference on Intelligent Transportation Systems, pp. 117-122. IEEE, 1997.

[68] Seiler, Pete, Aniruddha Pant, and Karl Hedrick. "Disturbance propagation in vehicle strings." IEEE Transactions on automatic control, vol. 49, no. 10, pp. 1835-1842, 2014.

[69] Li, Li, and Fei-Yue Wang. "Cooperative driving at blind crossings using intervehicle communication." IEEE Transactions on Vehicular technology, vol. 55, no. 6, pp. 1712-1724, 2016.

[70] Ksentini, A., H. Tounsi, and M. Frikha. "A proxy-based framework for QoS-enabled Internet access in VANETS." In The Second International Conference on Communications and Networking, vol. 1, no. 1, pp. 1-8. IEEE, 2010.

[71] Asefi, Mahdi, Sandra Céspedes, Xuemin Shen, and Jon W. Mark. "A seamless quality-driven multi-hop data delivery scheme for video streaming in urban VANET scenarios." In 2011 IEEE International Conference on Communications (ICC), vol. 1, no. 1, pp. 1-5. IEEE, 2011.

[72] Razzaq, Abdul, and Ahmed Mehaoua. "Video transport over VANETs: Multi-stream coding with multi-path and network coding." In IEEE Local Computer Network Conference, vol. 1, no. 1, pp. 32-39. IEEE, 2010.

[73] Lee, Chao-Hsien, Chung-Ming Huang, Chia-Ching Yang, and Tai-Hsiang Wang. "A cooperative video streaming system over the integrated cellular and DSRC networks." In 2011 IEEE Vehicular Technology Conference (VTC Fall),vol. 1, no. 1, pp. 1-5. IEEE, 2011.

[74] Seferoglu, Hulya, and Athina Markopoulou. "Opportunistic network coding for video streaming over wireless." In Packet Video 2007, pp. 191-200. IEEE, 2007.

[75] Kumar, Sushil, Upasana Dohare, Kirshna Kumar, Durga Prasad Dora, Kashif Naseer Qureshi, and Rupak Kharel. "Cybersecurity measures for geocasting in vehicular cyber physical system environments." IEEE Internet of Things Journal, vol. 6, no. 4, pp. 5916-5926, 2018.

[76] Wu, Weigang, Zhiwei Yang, and Keqin Li. "Internet of Vehicles and applications." In Internet of Things, pp. 299-317. Morgan Kaufmann, 2016.

[77] K. Z. Ghafoor, J. Lloret, K. A. Bakar, A. S. Sadiq, and S. A. B. Mussa, "Beaconing approaches in vehicular ad hoc networks: A survey," Wireless Personal Communications, vol. 73, no. 3, pp. 885–912, May 2013.

[78] G. P. Corser, H. Fu, and A. Banihani, "Evaluating location privacy in vehicular communications and applications," IEEE Transactions on Intelligent Transportation Systems, pp. 1–10, 2016.

[79] B. Ying, D. Makrakis, and H. T. Mouftah, "Dynamic mix-zone for location privacy in vehicular networks", IEEE Communications Letters, vol. 17, no. 8, pp.1524-1527, 2013.

[80] A. K. Tyagi, and N. Sreenath, April. "Location privacy preserving techniques for location based services over road networks", In Proceedings of ICCSP, IEEE, pp. 1319-1326, India, 2015.

[81] X. Huang, R. Yu, J. Kang, N. Wang, S. Maharjan and Y. Zhang, "Software Defined Networking With Pseudonym Systems for Secure Vehicular Clouds", IEEE Access, vol. 4, no.1, pp. 3522-3534, 2016.

[82] T. Yan, W. Zhang, and G. Wang, "A grid-based on-road localization system in VANET with linear error propagation," IEEE Transactions on Wireless Communications, vol. 13, no. 2, pp. 861–875, Feb. 2014.

[83] N. Alam, A. Tabatabaei Balaei, and A. G. Dempster, "Relative positioning enhancement in VANETs: A tight integration approach," IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 1, pp. 47–55, Mar. 2013.

[84] Yao, A. T. Balaei, M. Hassan, N. Alam, and A. G. Dempster, "Improving cooperative positioning for vehicular networks," IEEE Transactions on Vehicular Technology, vol. 60, no. 6, pp. 2810–2823, Jul. 2011.

[85] M. Fogue et al., "Securing warning message dissemination in VANETs using cooperative neighbor position verification," IEEE Transactions on Vehicular Technology, vol. 64, no. 6, pp. 2538–2550, Jun. 2015.

[86] M. Fogue, F. J. Martinez, P. Garrido, M. Fiore, C.F. Chiasserini, C. Casetti, J. C. Cano,C. T. Calafate, and P. Manzoni, "Securing warning message dissemination in VANETs using cooperative neighbor position verification", IEEE Transactions on Vehicular Technology, vol. 64, no. 6, pp.2538-2550, 2015.

[87] F. Malandrino, C. Borgiattino, C. Casetti, C. F. Chiasserini, M. Fiore, M. and R. Sadao,"Verification and inference of positions in vehicular networks through anonymous beaconing", IEEE Transactions on Mobile Computing, vol. 13, no. 10, pp.2415-2428, 2014.

[88] M. E. P. Monteiro, J.L. Rebelatto, and R. D. Souza, "Information-Theoretic LocationVerification System With Directional Antennas for Vehicular Networks", IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 1, pp. 93-103, 2016.

[89] T. Zhang, Securing Connected Vehicles: Challenges and Opportunities, CISCO Syst., San Jose, CA, USA, Dec. 2015. [Online]. Available: http://sites.ieee.org/ denver-com/files/2016/02/IoV-Security-Challenges and- Opportunities-zhang.pdf.

[90] D. Yadron, "Hackers demonstrate how to take control of cars," in Proc. Black Hat Security Conf., Las Vegas, NV, USA, 2015. [Online]. Available: http://www.wsj.com/articles/hacking-carsto-take-focus-at-black-hat-conference-1438723360?mod=videorelated..

[91] J. Hickey, Vice President, Vínsula. Telephone Interview, Seattle, WA, USA, Oct. 2012.

[92] L. Reger, Addressing the Security of the Connected Car,NXP Blog, Eindhoven, The Netherlands, 2014. [Online]. Available: http://blog.nxp.com/addressing-the-security-of-the-connected-car/.

[93] J. Hickey, Vice President, Vínsula. Telephone Interview, Seattle, WA, USA, Oct. 2012.

[94] National Institute of Standards and Technology (NIST): Framework for Improving Critical Infrastructure Cybersecurity. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[95] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, and B. Liu, "Practical secure and privacy-preserving scheme for value-added applications in VANETs," Comput.Commun., vol. 71, pp. 50–60, Nov. 2015.

[96] D. A. Rivas, J. M. Barceló-Ordinas, M. G. Zapata, and J. D. Morillo-Pozo, "Security on VANETs: Privacy, misbehaving nodes, false information, and secure data aggregation," J. Netw. Comput.Appl., vol. 34, no. 6, pp. 1942–1955, 2011.

[97] M. Saini, A. Alelaiwi, A. E and Saddik, "How close are we to Realizing a Pragmatic VANET Solution: A Meta-Survey," ACM Computing Surveys. Vol. 48, no. 2, p.29-65, 2015.

[98] S. F. Hasan, X. Ding, N. H. Siddique, and S. Chakraborty, "Measuring disruption in vehicular communications," IEEE transaction on Vehicular Technology, vol. 60, no. 1, pp.148-159, 2011.

[99] B. Aslam, P. Wang, and C. C. Zou, "Extension of internet access to VANET via satellite receive–only terminals," International Journal of Ad Hoc and Ubiquitous Computing, vol. 14, no. 3, pp.172-190, 2013.

[100] J. Toutouh, and E. Alba, "Light commodity devices for building vehicular ad hoc networks: An experimental study," Ad Hoc Networks, vol. 37, no. 1, pp.499-511, 2016.

[101] S. Bitam, A. Mellouk, and S. Zeadally, "VANET-cloud: a generic cloud computing model for vehicular Ad Hoc networks," IEEE Wireless Communications, vol. 22, no. 1, pp.96-102, 2015.

[102] W. Liang, Z. Li, H. Zhang, S. Wang, and R. Bie, "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends", International Journal of Distributed Sensor Networks, vol. 15, no.1, pp. 1-17, 2015.

[103] J. Barbaresso, G. Cordahi, D.e Garcia, C. Hill, A. Jendzejec and K. Wright, "USDOT's Intelligent Transportation Systems (ITS) ITS Strategic Plan 2015- 2019", Report: FHWA-JPO-14-145, US Department of Transportation Intelligent Transportation Systems, Joint Program Office.
Available: http://www.its.dot.gov/strategicplan/index.html.

[104] World Health Organization, "Global Status Report on Road Safety",pp. 1257,2015.
Available:
http://www.who.int/violence_injury_prevention/road_safety_status/2015/en/.

[105] International Road Assessment Programme, "Global Cost of Road Crash", 2013.
Available: http://www.irap.net/en/about-irap-3/research-and-technical-papers.

[106] European Environment Agency, "Assessment of Global Megatrends- States and Outlook", Report, 2015.
Available: http://www.eea.europa.eu/soer/europe-and-the-world/megatrends.

[107] Mckinsey & Company, "Mobility of the future", 2013. Available:
http://www.mckinsey.com/client_service/automotive_and_assembly/latest_thinking.

[108] Govt. of UK Govt. "The Internet of Things: Making the most of second digital revolution", Report, 2014. Available:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.

[109] Gartner, "Internet of Things Units Installed Base by Category", 2014
Available: http://www.gartner.com/newsroom/id/2905717.

[110] Mckinsey & Company, "Unlocking the potential of the Internet of Things"2015.
Available:
http://www.mckinsey.com/insights/business_technology/the_internet_of_things_the_value_of_digitizing_the_physical_world/.

[111] K. N. Qureshi, S. Din, G. Jeon and F. Piccialli, "Internet of Vehicles: Key Technologies, Network Model, Solutions and Challenges With Future Aspects," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 3, pp. 1777-1786, March 2021.

[112] M. Chen, Y. Tian, G. Fortino, J. Zhang, and I. Humar, "Cognitive Internet of vehicles," Comput. Commun., vol. 120, pp. 58–70, May 2018.

[113] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran, and K. Zhou, "Mobile crowd sensing for traffic prediction in Internet of vehicles," Sensors, vol. 16, no. 1, p. 88, Jan. 2016.

[114] M. A. Salahuddin, A. Al-Fuqaha, and M. Guizani, "Software-defined networking for rsu clouds in support of the Internet of vehicles," IEEE Internet Things J., vol. 2, no. 2, pp. 133–144, Apr. 2015.

[115] Lu, Zhaojun, Wenchao Liu, Qian Wang, Gang Qu, and Zhenglin Liu. "A privacy-preserving trust model based on blockchain for VANETs." IEEE Access, vol. 6, no. 1, pp. 45655-45664, 2018.

[116] Sakiz, Fatih, and Sevil Sen. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV." Ad Hoc Networks, vol. 61, no. 1, pp. 33-50, 2017.

[117] Chauhan, Kamal Kumar, Sumit Kumar, and Suresh Kumar. "The design of a secure key management system in vehicular ad hoc networks." In 2017 conference on information and communication technology (CICT), vol. 1, no. 1, pp. 1-6. IEEE, 2017.

[118] Azees, Maria, Pandi Vijayakumar, and Lazarus Jegatha Deborah. "Comprehensive survey on security services in vehicular ad-hoc networks." IET Intelligent Transport Systems, vol. 10, no. 6, pp. 379-388, 2016.

[119] Mokhtar, Bassem, and Mohamed Azab. "Survey on security issues in vehicular ad hoc networks." Alexandria engineering journal, vol. 54, no. 4, pp. 1115-1126, 2015.

[120] K. Golestan, R. Soua, F. Karray, and M. Kamel, "Situation awareness within the context of connected cars: A comprehensive review and recent trends," Inf. Fusion, vol. 29, pp. 6–83, May 2016.

[121] Nanjie, L., Internet of Vehicles your next connection.WinWin Magazine, Issue 11, HUAWEI, 2011.

[122] Wan, Jiafu, Daqiang Zhang, Shengjie Zhao, Laurence T. Yang, and Jaime Lloret. "Context-aware vehicular cyber-physical systems with cloud support: architecture, challenges, and solutions." IEEE Communications Magazine, vol. 52, no. 8, pp. 106-113, 2014.

[123] Liu, N. "Internet of Vehicles: Your next connection." Huawei WinWin, vol. 11, no. 1, pp. 23-28, 2011.

[124] B. Anitha and K. Duraiswamy, ‘‘A heuristic moving vehicle location prediction technique via optimal paths selection with aid of genetic algorithm and feed forward back propagation neural network,’’ Int. J. Comput. Science, vol. 8, no. 12, pp. 2008–2016, Dec. 2012

[125] F. Oliveira, D. G. Costa, C. Duran-Faundez and A. Dias, "BikeWay: A Multi-Sensory Fuzzy-Based Quality Metric for Bike Paths and Tracks in Urban Areas," in IEEE Access, vol. 8, pp. 227313-227326, 2020.

[126] Yaqub, Muhammad Azfar, Syed Hassan Ahmed, and Dongkyun Kim. "Asking neighbors a favor: Cooperative video retrieval using cellular networks in VANETs." Vehicular Communications, vol. 12, no. 1, pp. 39-49, 2018.

[127] Junior, Wellington Lobato, Denis Rosário, Eduardo Cerqueira, Leandro A. Villas, and Mario Gerla. "A game theory approach for platoon-based driving for multimedia transmission in VANETs." Wireless Communications and Mobile Computing 2018 (2018).

[128] Medeiros, Iago, Wellington Lobato Junior, Denis Rosário, Eduardo Cerqueira, Torsten Braun, and Leandro A. Villas. "A comparative analysis of platoon-based driving protocols for video dissemination over VANETs." In 2018 IEEE International Conference on Communications Workshops (ICC Workshops), pp. 1-5. IEEE, 2018.

[129] Wang, Mu, Changqiao Xu, Shijie Jia, Jianfeng Guan, and Luigi Alfredo Grieco. "Preference-aware fast interest forwarding for video streaming in information-centric

VANETs." In 2017 IEEE International Conference on Communications (ICC), pp. 1-7. IEEE, 2017.

[130] Sermpezis, Pavlos, Georgios Koltsidas, and Fotini-Niovi Pavlidou. "Investigating a junction-based multipath source routing algorithm for VANETs." IEEE Communications letters, vol. 17, no. 3, pp. 600-603, 2013.

[131] Salkuyeh, Mostafa Asgharpoor, and Bahman Abolhassani. "An adaptive multipath geographic routing for video transmission in urban VANETs." IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 10, pp. 2822-2831, 2016.

[132] De Felice, Mario, Eduardo Cerqueira, Adalberto Melo, Mario Gerla, Francesca Cuomo, and Andrea Baiocchi. "A distributed beaconless routing protocol for real-time video dissemination in multimedia VANETs." Computer communications, vol. 58, no. 1, pp.b40-52, 2015.

[133] Wu, Honghai, and Huadong Ma. "Opportunistic routing for live video streaming in vehicular ad hoc networks." In Proceeding of IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks 2014, pp. 1-3. IEEE, 2014.

[134] Wang, Renfei, Mohammed Almulla, Cristiano Rezende, and Azzedine Boukerche. "Video streaming over vehicular networks by a multiple path solution with error correction." In 2014 IEEE International Conference on Communications (ICC), pp. 580-585. IEEE, 2014.

[135] Al-Ani, Aymen, and Jochen Seitz. "QoS-aware routing for video streaming in multi-rate Ad hoc Networks." In 2016 9th IFIP Wireless and mobile networking conference (WMNC), pp. 193-198. IEEE, 2016.

[136] Quadros, Carlos, Aldri Santos, Mario Gerla, and Eduardo Cerqueira. "QoE-driven dissemination of real-time videos over vehicular networks." Computer Communications, vol. 9, no. 1, pp. 133-147, 2016.

[137] Sampigethaya, Krishna, Mingyan Li, Leping Huang, and Radha Poovendran. "AMOEBA: Robust location privacy scheme for VANET." IEEE Journal on Selected Areas in communications, vol. 25, no. 8, pp. 1569-1589, 2007

[138] Emara, Karim, Wolfgang Woerndl, and Johann Schlichter. "Context-aware privacy scheme for VANET safety applicationschemes for VANET safety applications." Computer Communications, vol. 63, no. 1, pp. 11-23, 2015

[139] Mei, Ying, Guozhou Jiang, Wei Zhang, and Yongquan Cui. "A collaboratively hidden location privacy scheme for VANETs." International Journal of Distributed Sensor Networks, vol. 10, no. 3, pp. 473151-473169, 2014.

[140] Kaushik, Sapna S. "Review of different approaches for privacy scheme in VANETs." International Journal of Advances in Engineering & Technology, vol. 5, no. 2, pp. 356-368, 2013.

[141] Song, Joo-Han, Vincent WS Wong, and Victor CM Leung. "Wireless location privacy protection in vehicular ad-hoc networks." Mobile Networks and Applications, vol. 15, no. 1, pp. 160-171, 2010.

[142] Al-ani, Ruqayah, Bo Zhou, Qi Shi, Thar Baker, and Mohamed Abdlhamed. "Adjusted location privacy scheme for VANET safety applications." In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, vol. 1, no. 1, pp. 1-4. IEEE, 2020.

[143] Zhang, Chuan, Liehuang Zhu, Chang Xu, Kashif Sharif, Kai Ding, Ximeng Liu, Xiaojiang Du, and Mohsen Guizani. "TPPR: A trust-based and privacy-preserving platoon recommendation scheme in VANET." IEEE Transactions on Services Computing (2019).

[144] Ghane, Soheila, Alireza Jolfaei, Lars Kulik, Kotagiri Ramamohanarao, and Deepak Puthal. "Preserving privacy in the internet of connected vehicles." IEEE Transactions on Intelligent Transportation Systems (2020).

[145] Ali, Qazi Ejaz, Naveed Ahmad, Abdul Haseeb Malik, Gauhar Ali, and Waheed Ur Rehman. "Issues, challenges, and research opportunities in intelligent transport system for security and privacy." Applied Sciences, vol. 8, no. 10, pp. 1964-1978, 2018.

[146] Cheng, Jiujun, Huaichen Yan, Aiguo Zhou, Chunmei Liu, Ding Cheng, Shangce Gao, Di Zang, and Deli Cheng. "Location prediction model based on the Internet of vehicles for assistance to medical vehicles." IEEE Access, vol. 8, no. 1, pp. 10754-10767, 2019.

[147] Ortiz, Michaël Garcia, Franz Kummert, and Jens Schmüdderich. "Prediction of driver behavior on a limited sensory setting." In 2012 15th International IEEE Conference on Intelligent Transportation Systems, vol. 1, no. 1, pp. 638-643. IEEE, 2012.

[148] A. Bohlooli and K. Jamshidi, ‘‘A GPS-free method for vehicle future movement directions prediction using SOM for VANET,’’ Appl. Intell., vol. 36, no. 3, pp. 685–697, Apr. 2011.

[149] B. Anitha and K. Duraiswamy, ‘‘A heuristic moving vehicle location prediction technique via optimal paths selection with aid of genetic algorithm and feed forward back propagation neural network,’’ Int. J. Comput. Science., vol. 8, no. 12, pp. 2008–2016, Dec. 2012.

[150] F. Oliveira, D. G. Costa, C. Duran-Faundez and A. Dias, "BikeWay: A Multi-Sensory Fuzzy-Based Quality Metric for Bike Paths and Tracks in Urban Areas," in IEEE Access, vol. 8,no. 1, pp. 227313-227326, 2020.

[151] Zadeh, Lotfi A. "Soft computing, fuzzy logic and recognition technology." In 1998 IEEE International Conference on Fuzzy Systems Proceedings. IEEE World Congress on Computational Intelligence (Cat. No. 98CH36228), vol. 2, pp. 1678-1679. IEEE, 1998.

[152] Mamdani, Ebrahim H. "Application of fuzzy logic to approximate reasoning using linguistic synthesis." IEEE transactions on computers, vol. 26, no. 12, pp. 1182-1191, 1997.

[153] L. Nie, Z. Ning, X. Wang, X. Hu, J. Cheng and Y. Li, "Data-Driven Intrusion Detection for Intelligent Internet of Vehicles: A Deep Convolutional Neural Network-Based Method," in IEEE Transactions on Network Science and Engineering, vol. 7, no. 4, pp. 2219-2230, Dec 2020.

[154] Y. Zhang, J. Li, Y. Guo, C. Xu, J. Bao and Y. Song, "Vehicle Driving Behavior Recognition Based on Multi-View Convolutional Neural Network With Joint Data Augmentation," in IEEE Transactions on Vehicular Technology, vol. 68, no. 5, pp. 4223-4234, May 2019.

[155] Arooj, Ansif, Muhammad Shoaib Farooq, Tariq Umer, Ghulam Rasool, and Bo Wang. "Cyber physical and social networks in IoV (CPSN-IoV): a multimodal architecture in edge-based networks for optimal route selection using 5G technologies." IEEE Access, vol. 8, no. 1, pp. 33609-33630, 2020.

[156] Arooj, Ansif, Muhammad Shoaib Farooq, Tariq Umer, Ghulam Rasool, and Bo Wang. "Cyber physical and social networks in IoV (CPSN-IoV): a multimodal architecture in edge-based networks for optimal route selection using 5G technologies." IEEE Access, vol. 8, no. 1, pp. 33609-33630, 2020.

[157] Wex, Philipp, Jochen Breuer, Albert Held, Tim Leinmuller, and Luca Delgrossi. "Trust issues for vehicular ad hoc networks." In VTC Spring 2008-IEEE Vehicular Technology Conference, pp. 2800-2804. IEEE, 2008.

[158] Sumra, Irshad Ahmed, Halabi Bin Hasbullah, A. Manan, and J. L. Bin. "Comparative study of security hardware modules (EDR, TPD and TPM) in VANET." In Proc. 3rd Nat. Inf. Technol. Symp.(NITS),vol. 1, no. 1, pp. 6-9. 2011.

[159] Brickell, Ernie, Jan Camenisch, and Liqun Chen. "Direct anonymous attestation." In Proceedings of the 11th ACM conference on Computer and communications security, vol. 1, no. 1, pp. 132-145. 2004.

[160] van den Berg, Eric, Tao Zhang, and Stanley Pietrowicz. "Blend-in: a privacy-enhancing certificate-selection method for vehicular communication." IEEE transactions on vehicular technology, vol. 58, no. 9, pp. 5190-5199, 2009.

[161] Boneh, Dan, Xavier Boyen, and Hovav Shacham. "Short group signatures." In Annual international cryptology conference, Springer, Berlin, Heidelberg, pp. 41-55. 2004.

[162] Lin, Xiaodong, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. "GSIS: A secure and privacy-preserving protocol for vehicular communications." IEEE Transactions on vehicular technology, vol. 56, no. 6, pp. 3442-3456, 2007.

[163] Xiong, Hu, Guobin Zhu, Zhong Chen, and Fagen Li. "Efficient communication scheme with confidentiality and privacy for vehicular networks." Computers & Electrical Engineering, vol. 39, no. 6, pp. 1717-1725, 2013.

[164] Huang, Jiun-Long, Lo-Yao Yeh, and Hung-Yu Chien. "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks." IEEE Transactions on Vehicular Technology, vol. 60, no. 1, pp. 248-262, 2010.

[165] Raya, Maxim, Panagiotis Papadimitratos, Imad Aad, Daniel Jungels, and Jean-Pierre Hubaux. "Eviction of misbehaving and faulty nodes in vehicular networks." IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1557-1568, 2007.

[166] Rivest, Ronald L., Adi Shamir, and Yael Tauman. "How to leak a secret: Theory and applications of ring signatures." In Theoretical Computer Science, pp. 164-186. Springer, Berlin, Heidelberg, 2006.

[167] Xiong, Hu, Konstantin Beznosov, Zhiguang Qin, and Matei Ripeanu. "Efficient and spontaneous privacy-preserving protocol for secure vehicular communication." In 2010 IEEE International Conference on Communications, pp. 1-6. IEEE, 2010.

[168] Xiong, Hu, Zhong Chen, and Fagen Li. "Efficient and multi-level privacy-preserving communication protocol for VANET." Computers & Electrical Engineering, vol. 38, no. 3, pp. 573-581, 2012.

[169] S. Garg, K. Kaur, G. Kaddoum, S. H. Ahmed, and D. N. K. Jayakody, "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective," IEEE Trans. Veh. Technol., vol. 68, no. 9,pp. 8421–8434, Sep. 2019.

[170] J. Gao et al., "A Blockchain-SDN-Enabled Internet of Vehicles Environment for Fog Computing and 5G Networks," in IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4278-4291, May 2020.

[171] Y. Chen, Z. Lu, H. Xiong, and W. Xu, "Privacy-preserving data aggregation protocol for fog computing-assisted vehicle-to-infrastructure scenario," Security and Communication Networks, vol. 2018, Article ID1378583, 14 pages, 2018.

[172] Sheet, Dalya Khalid, Omprakash Kaiwartya, Abdul Hanan Abdullah, Yue Cao, Ahmed Nazar Hassan, and Sushil Kumar. "Location information verification using transferable belief model for geographic routing in vehicular ad hoc networks." IET Intelligent Transport Systems, vol.11, no. 2, pp. 53-60, 2017.

[173] Qureshi, Kashif Naseer, Abdul Hanan Abdullah, Omprakash Kaiwartya, Fasee Ullah, Saleem Iqbal, and Ayman Altameem. "Weighted link quality and forward progress coupled with modified RTS/CTS for beaconless packet forwarding protocol (B-PFP) in VANETs." Telecommunication Systems, vol. 75, no. 2, pp. 145-160, 2016.

[174] Wang, Lu, Hailiang Yang, Xiaoke Qi, Jun Xu, and Kaishun Wu. "ICast: Fine-grained wireless video streaming over Internet of intelligent vehicles." IEEE Internet of Things Journal,vol. 6, no. 1, pp. 111-123, 2018.

[175] Qureshi, Kashif Naseer, Abdul Hanan Abdullah, Omprakash Kaiwartya, Saleem Iqbal, Rizwan Aslam Butt, and Faisal Bashir. "A Dynamic Congestion Control Scheme for safety applications in vehicular ad hoc networks." Computers & Electrical Engineering, vol. 72, no. 1, pp. 774-788, 2018.

[176] Hossain, Tareq, Yi Cui, and Yuan Xue. "Vanets: Case study of a peer-to-peer video conferencing system." In 2009 6th IEEE Consumer Communications and Networking Conference, pp. 1-2. IEEE, 2009.

[177] Kaiwartya, Omprakash, Abdul Hanan Abdullah, Yue Cao, Jaime Lloret, Sushil Kumar, Rajiv Ratn Shah, Mukesh Prasad, and Shiv Prakash. "Virtualization in wireless sensor networks: Fault tolerant embedding for internet of things." IEEE Internet of Things Journal, vol. 5, no. 2, pp. 571-580, 2017.

[178] Aliyu, Ahmed, Abdul Hanan Abdullah, Omprakash Kaiwartya, Fasee Ullah, Usman M. Joda, and Ahmed Nazar Hassan. "Multi-Path video streaming in vehicular communication: Approaches and challenges." In 2017 6th ICT International Student Project Conference (ICT-ISPC), pp. 1-4. IEEE, 2017.

[179] Cao, Yue, Omprakash Kaiwartya, Nauman Aslam, Chong Han, Xu Zhang, Yuan Zhuang, and Mehrdad Dianati. "A trajectory-driven opportunistic routing protocol for VCPS." IEEE Transactions on Aerospace and Electronic Systems, vol. 54, no. 6, pp. 2628-2642, 2018.

[180] Xie, Hengheng, Azzedine Boukerche, and Antonio AF Loureiro. "A multipath video streaming solution for vehicular networks with link disjoint and node-disjoint." IEEE

Transactions on Parallel and Distributed Systems, vol. 26, no. 12, pp. 3223-3235, 2014.

[181] Aliyu, Ahmed, Abdul Hanan Abdullah, Ajay Sikandar, Usman M. Joda, Fatai I. Sadiq, and Abubakar Ado. "Minimizing Route Coupling Effect in Multipath Video Streaming Over Vehicular Network." In International Conference on Application of Computing and Communication Technologies, pp. 139-151. Springer, Singapore, 2018.

[182] De Felice, Mario, Eduardo Cerqueira, Adalberto Melo, Mario Gerla, Francesca Cuomo, and Andrea Baiocchi. "A distributed beaconless routing protocol for real-time video dissemination in multimedia VANETs." Computer communications 58 (2015): 40-52.

[183] Kasana, Reena, Sushil Kumar, Omprakash Kaiwartya, Rupak Kharel, Jaime Lloret, Nauman Aslam, and Tong Wang. "Fuzzy-based channel selection for location oriented services in multichannel VCPS environments." IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4642-4651, 2018.

[184] Kaiwartya, Omprakash, and Sushil Kumar. "Geocast routing: Recent advances and future challenges in vehicular adhoc networks." In 2014 International Conference on Signal Processing and Integrated Networks (SPIN), pp. 291-296. IEEE, 2014.

[185] Kaiwartya, Omprakash, and Sushil Kumar. "Guaranteed geocast routing protocol for vehicular adhoc networks in highway traffic environment." Wireless Personal Communications, vol. 83, no. 4, pp. 2657-2682, 2015.

[186] Khasawneh, Ahmad, Muhammad Shafie Bin Abd Latiff, Hassan Chizari, MoeenUddin Tariq, and Abdullah Bamatraf. "Pressure based routing protocol for underwater wireless sensor networks: A survey." KSII Transactions on Internet and Information Systems (TIIS), vol. 9, no. 2, pp. 504-527, 2015.

[187] Darwish, Tasneem, and Kamalrulnizam Abu Bakar. "Traffic aware routing in vehicular ad hoc networks: characteristics and challenges." Telecommunication systems, vol. 61, no. 3, pp. 489-513, 2016.

[188] Qureshi, Kashif Naseer, Abdul Hanan Abdullah, Jaime Lloret, and Ayman Altameem. "Road-aware routing strategies for vehicular ad hoc networks: Characteristics and

comparisons." International Journal of Distributed Sensor Networks, vol. 12, no. 3, pp. 1605734, 2016.

[189] Lai, Wei Kuang, Chih Kun Tai, Tin-Yu Wu, Alagan Anpalagan, and Jian Zhi Chen. "PBMP: priority-based multi-path packet routing for vehicular ad hoc network system in city environment." Transactions on Emerging Telecommunications Technologies, vol. 27, no. 10, pp. 1331-1344, 2016.

[190] Immich, Roger, Eduardo Cerqueira, and Marilia Curado. "Shielding video streaming against packet losses over VANETs." Wireless Networks, vol. 22, no. 8, pp. 2563-2577, 2016.

[191] Yang, Zhenyu, Ming Li, and Wenjing Lou. "Codeplay: Live multimedia streaming in vanets using symbol-level network coding." In The 18th IEEE International Conference on Network Protocols, pp. 223-232. IEEE, 2010.

[192] Zaidi, Sofiane, Salim Bitam, and Abdelhamid Mellouk. "Hybrid error recovery protocol for video streaming in vehicle ad hoc networks." Vehicular communications, vol. 12, no. 1, pp. 110-126, 2018.

[193] Yin, Bo, and Xuetao Wei. "Communication-efficient data aggregation tree construction for complex queries in IoT applications." IEEE Internet of Things Journal, vol. 6, no. 2, pp. 3352-3363, 2018.

[194] Wang, Jin, Yu Gao, Wei Liu, Arun Kumar Sangaiah, and Hye-Jin Kim. "Energy efficient routing algorithm with mobile sink support for wireless sensor networks." Vol. 19, no. 7, pp. 1494-1508, 2019.

[195] Wang, Jin, Yu Gao, Wei Liu, Arun Kumar Sangaiah, and Hye-Jin Kim. "An improved routing schema with special clustering using PSO algorithm for heterogeneous wireless sensor network." Vol. 19, no. 3, pp. 671-684, 2019.

[196] Wang, Jin, Jiayi Cao, R. Simon Sherratt, and Jong Hyuk Park. "An improved ant colony optimization-based approach with mobile sink for wireless sensor networks." The Journal of Supercomputing, vol. 74, no. 12, pp. 6633-6645, 2019.

[197] Tang, Qiang, Mingzhong Xie, Kun Yang, Yuansheng Luo, Dongdai Zhou, and Yun Song. "A decision function based smart charging and discharging strategy for electric

vehicle in smart grid." Mobile Networks and Applications, vol. 24, no. 5, pp.1722-1731, 2019.

[198] Rashidi, Maryam, Iulian Batros, Tatiana K. Madsen, Muhammad T. Riaz, and Thomas Paulin. "Placement of road side units for floating car data collection in highway scenario." In 2012 IV International Congress on Ultra Modern Telecommunications and Control Systems, pp. 114-118. IEEE, 2012.

[199] Emara, Karim, Wolfgang Woerndl, and Johann Schlichter. "On evaluation of location privacy preserving schemes for VANET safety applications." Computer Communications, vol. 63, no. 1, pp. 11-23, 2015.

[200] Emara, Karim, Wolfgang Woerndl, and Johann Schlichter. "CAPS: Context-aware privacy scheme for VANET safety applications." In Proceedings of the 8th ACM conference on security & privacy in wireless and mobile networks, pp. 1-12. 2015.

[201] Zidani, Ferroudja, Fouzi Semchedine, and Marwane Ayaida. "Estimation of Neighbors Position privacy scheme with an Adaptive Beaconing approach for location privacy in VANETs." Computers & Electrical Engineering, vol. 71, no. 1, pp. 359-371,2018.

[202] Wasef, Albert, and Xuemin Sherman Shen. "REP: Location privacy for VANETs using random encryption periods." Mobile Networks and Application, vol. 15, no. 1, pp. 172-185, 2010.

[203] Chen, Yi-Ming, and Yu-Chih Wei. "SafeAnon: a safe location privacy scheme for vehicular networks." Telecommunication Systems, vol. 50, no. 4, pp. 339-354, 2014.

[204] Lu, Rongxing, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, and Xuemin Shen. "Pseudonym changing at social spots: An effective strategy for location privacy in vanets." IEEE transactions on vehicular technology, vol. 61, no. 1, pp. 86-96, 2011.

[205] Emara, Karim. "Safety-aware location privacy in VANET: Evaluation and comparison." IEEE Transactions on Vehicular Technology, vol. 66, no. 12, pp. 10718-10731, 2017.

[206] Mei, Ying, Guozhou Jiang, Wei Zhang, and Yongquan Cui. "A collaboratively hidden location privacy scheme for VANETs." International Journal of Distributed Sensor Networks, vol. 10, no. 3, pp. 473-489, 2014.

[207] Song, Joo-Han, Vincent WS Wong, and Victor CM Leung. "Wireless location privacy protection in vehicular ad-hoc networks." Mobile Networks and Applications, vol. 15, no. 1, pp. 160-171, 2010.

[208] Chen, Yi-Ming, and Yu-Chih Wei. "A beacon-based trust management system for enhancing user centric location privacy in VANETs." Journal of Communications and Networks, vol. 15, no. 2, pp. 153-163, 2013.

[209] Eckhoff, D., Sommer, C., Gansen, T., German, R. and Dressler, F., 2010, December. Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping. In 2010 IEEE Vehicular Networking Conference (pp. 174-181). IEEE.

[210] Taha, Sanaa, and Xuemin Shen. "A physical-layer location privacy-preserving scheme for mobile public hotspots in NEMO-based VANETs." IEEE Transactions on Intelligent Transportation Systems, vol. 14, no. 4, pp. 1665-1680, 2013.

[211] Sun, Yipin, Bofeng Zhang, Baokang Zhao, Xiangyu Su, and Jinshu Su. "Mix-zones optimal deployment for protecting location privacy in VANET." Peer-to-Peer Networking and Applications, vol. 8, no. 6, pp. 1108-1121, 2015.

[212] Kaushik, Sapna S. "Review of different approaches for privacy scheme in VANETs." International Journal of Advances in Engineering & Technology, vol. 5, no. 2, pp. 356-378, 2013.

[213] Al-ani, Ruqayah, Bo Zhou, Qi Shi, Thar Baker, and Mohamed Abdlhamed. "Adjusted location privacy scheme for VANET safety applications." In NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, pp. 1-4. IEEE, 2020.

[214] Khacheba, Ines, Mohamed B. Yagoubi, Nasreddine Lagraa, and Abderrahmane Lakas. "CLPS: context-based location privacy scheme for VANETs." International Journal of Ad Hoc and Ubiquitous Computing, vol. 29, no. 1-2, pp. 141-159, 2018.

[215] Manvi, Sunilkumar S., and Shrikant Tangade. "A survey on authentication schemes in VANETs for secured communication." Vehicular Communications, vol. 9, no. 1, pp. 19-30, 2017.

[216] Sheikh, Muhammad Sameer, Jun Liang, and Wensong Wang. "A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)." Sensors, vol. 19, no. 16, pp. 3589-3604, 2019.

[217] Sheikh, Muhammad Sameer, Jun Liang, and Wensong Wang. "Security and privacy in vehicular ad hoc network and vehicle cloud computing: a survey." Wireless Communications and Mobile Computing 2020 (2020).

[218] Ogundoyin, Sunday Oyinlola. "An Efficient, Secure and Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad-hoc Networks." Journal of Information Assurance & Security, vol. 12, no. 5, pp. 201-218, 2017.

[219] Zhang, Chuan, Liehuang Zhu, Chang Xu, Kashif Sharif, Kai Ding, Ximeng Liu, Xiaojiang Du, and Mohsen Guizani. "TPPR: A trust-based and privacy-preserving platoon recommendation scheme in VANET." IEEE Transactions on Services Computing (2019).

[220] Ghane, Soheila, Alireza Jolfaei, Lars Kulik, Kotagiri Ramamohanarao, and Deepak Puthal. "Preserving privacy in the internet of connected vehicles." IEEE Transactions on Intelligent Transportation Systems (2020).

[221] Ali, Qazi Ejaz, Naveed Ahmad, Abdul Haseeb Malik, Gauhar Ali, and Waheed Ur Rehman. "Issues, challenges, and research opportunities in intelligent transport system for security and privacy." Applied Sciences, vol. 8, no. 10, pp. 1964-2978, 2019.

[222] Liu, Zhi-Cai, Ling Xiong, Tu Peng, Dai-Yuan Peng, and Hong-Bin Liang. "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks." IEEE Access, vol. 6, no. 1, pp. 26307-26317, 2018.

[223] Zhong, Hong, Shunshun Han, Jie Cui, Jing Zhang, and Yan Xu. "Privacy-preserving authentication scheme with full aggregation in VANET." Information Sciences 476, vol. 1, no. 1, pp. 211-221, 2019.

[224] A. Wasef and X. Shen, “Emap: Expedite message authentication protocol for vehicular ad hoc networks,” IEEE transactions on Mobile Computing, vol. 12, no. 1, pp. 78–89, 2011.

[225] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2740–2749, 2017.

[226] M. Ma, D. He, H. Wang, N. Kumar, and K.-K. R. Choo, "An efficient and provably secure authenticated key agreement protocol for fog-based vehicular ad-hoc networks," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 8065–8075, 2019.

[227] O. Kaiwartya et al., "Geometry-Based Localization for GPS Outage in Vehicular Cyber Physical Systems," in IEEE Transactions on Vehicular Technology, vol. 67, no. 5, pp. 3800-3812, May 2018.

[228] Rathee, Priyanka, Rishipal Singh, and Sushil Kumar. "Performance Analysis of IEEE 802.11 p in the Presence of Hidden Terminals." Wireless Personal Communications, vol. 89, no. 1, pp. 61-78, 2016.

[229] Liu, Yanbing, Yuhang Wang, and Guanghui Chang. "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm." IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 10, pp. 2740-2749, 2017.

[230] Sakiz, Fatih, and Sevil Sen. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV." Ad Hoc Networks, vol. 61, no. 1, pp. 33-50, 2017.

[231] Bao, Shihan, Yue Cao, Ao Lei, Philip Asuquo, Haitham Cruickshank, Zhili Sun, and Michael Huth. "Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems." IEEE Access, vol. 7, no. 1, pp. 80390-80403, 2019.

[232] Chen, Yin Ru, Jin Rui Sha, and Zhi Hong Zhou. "IOV Privacy Protection System Based on Double-Layered Chains." Wireless Communications and Mobile Computing 2019 (2019).

[233] Hussain, Rasheed, Fizza Abbas, Junggab Son, Donghyun Kim, Sangjin Kim, and Heekuck Oh. "Vehicle witnesses as a service: Leveraging vehicles as witnesses on the

road in vanet clouds." In 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, vol. 1, pp. 439-444. IEEE, 2013.

[234] He, Wu, Gongjun Yan, and Li Da Xu. "Developing vehicular data cloud services in the IoT environment." IEEE transactions on industrial informatics, vol. 10, no. 2, pp. 1587-1595, 2014.

[235] Bharat, M., K. Santhi Sree, and T. Mahesh Kumar. "Authentication solution for security attacks in VANETs." International Journal of Advanced Research in Computer and Communication Engineering, vol. 3, no. 8, pp. 2278-1021, 2014.

[236] Li, Hongwei, Rongxing Lu, Liang Zhou, Bo Yang, and Xuemin Shen. "An efficient merkle-tree-based authentication scheme for smart grid." IEEE Systems Journal, vol.8, no. 2, pp. 655-663, 2013.

[237] Farash, Mohammad Sabzinejad, Muhamed Turkanović, Saru Kumari, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment." Ad Hoc Networks, vol. 36, no. 1, pp. 152-176, 2016.

[238] Li, Hongwei, Dongxiao Liu, Yuanshun Dai, and Tom H. Luan. "Engineering searchable encryption of mobile cloud networks: When QoE meets QoP." IEEE Wireless Communications, vol. 22, no. 4, pp.74-80, 2015.

[239] Garg, Sahil, Kuljeet Kaur, Georges Kaddoum, Syed Hassan Ahmed, and Dushantha Nalin K. Jayakody. "SDN-based secure and privacy-preserving scheme for vehicular networks: A 5G perspective." IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 8421-8434, 2019.

[240] Gao, Jianbin, Kwame Opuni-Boachie Obour Agyekum, Emmanuel Boateng Sifah, Kingsley Nketia Acheampong, Qi Xia, Xiaojiang Du, Mohsen Guizani, and Hu Xia. "A blockchain-SDN-enabled Internet of vehicles environment for fog computing and 5G networks." IEEE Internet of Things Journal, vol. 7, no. 5, pp. 4278-4291, 2019.

[241] Arooj, Ansif, Muhammad Shoaib Farooq, Tariq Umer, Ghulam Rasool, and Bo Wang. "Cyber physical and social networks in IoV (CPSN-IoV): a multimodal architecture in

edge-based networks for optimal route selection using 5G technologies." IEEE Access, vol. 8, pp. 33609-33630, 2020.

[242] Park, Joon-Sang, and Seung Jun Beak. "Securing one-way hash chain based incentive mechanism for vehicular ad hoc networks." Peer-to-Peer Networking and Applications, vol. 7, no. 4, pp. 737-742, 2014.

[243] Lee, Suk-Bok, Joon-Sang Park, Mario Gerla, and Songwu Lu. "Secure incentives for commercial ad dissemination in vehicular networks." IEEE Transactions on Vehicular Technology, vol. 61, no. 6, pp. 2715-2728, 2012.

[244] Li, Feng, and Jie Wu. "Frame: An innovative incentive scheme in vehicular networks." In 2009 IEEE International Conference on Communications, pp. 1-6. IEEE, 2009.

[245] Tseng, Fu-Kuo, Yung-Hsiang Liu, Jing-Shyang Hwu, and Rong-Jaye Chen. "A secure reed–solomon code incentive scheme for commercial ad dissemination over VANETs." IEEE Transactions on Vehicular Technology, vol. 60, no. 9, pp. 4598-4608, 2011.

[246] Li, Qinghua, and Guohong Cao. "Providing privacy-aware incentives for mobile sensing." In 2013 IEEE international conference on pervasive computing and communications (PerCom), pp. 76-84. IEEE, 2013.

[247] de Fuentes, Jose Maria, Jorge Blasco, Ana Isabel González-Tablas, and Lorena González-Manzano. "Applying information hiding in VANETs to covertly report misbehaving vehicles." International Journal of Distributed Sensor Networks, vol. 10, no. 2, pp.120-136, 2014.