Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issues 3, pp. 425–440, DOI 10.12694:/scpe.v21i3.1741

INTERNET OF VEHICLES (IOV) OVER VANETS: SMART AND SECURE COMMUNICATION USING IOT

SUMIT KUMAR* AND JASPREET SINGH†

Abstract. The new age of the Internet of Things (IoT) is motivating the advancement of traditional Vehicular Ad-Hoc Networks (VANETs) into the Internet of Vehicles (IoV). This paper is an overview of smart and secure communications to reduce traffic congestion using IoT based VANETs, known as IoV networks. Studies and observations made in this paper suggest that the practice of combining IoT and VANET for a secure combination has rarely practiced. IoV uses real-time data communication between vehicles to everything (V2X) using wireless communication devices based on fog/edge computing; therefore, it has considered as an application of Cyber-physical systems (CPS). Various modes of V2X communication with their connecting technologies also discussed. This paper delivers a detailed introduction to the Internet of Vehicles (IoV) with current applications, discusses the architecture of IoV based on currently existing communication technologies and routing protocols, presenting different issues in detail, provides several open research challenges and the trade-off between security and privacy in the area of IoV has reviewed. From the analysis of previous work in the IoV network, we concluded the utilization of artificial intelligence and machine learning concept is a beneficial step toward the future of IoV model.

Key words: IoT, VANET, IoV, Secure communication, Traffic congestion, Artificial Intelligence techniques, Cyber-physical systems (CPS)

AMS subject classifications. 68M11

1. Introduction. The Internet of Things (IoT) refers to physical devices equipped with sensors, such as smart wearables, autonomous vehicles, mobile phones, home appliances, machines, and other electronic devices connected via an application programming interface (API) for data transmission over the Internet [1]. When vehicles are connected to the Internet and act as an ad-hoc network, it is known as the Internet of Vehicles (IoV). It is emerging as an innovative model in the wireless and mobile communications sectors with a resolution of new communication and connectivity technologies assisted by the development of IoT [2]. Vehicular Ad-hoc network (VANET) gave rise to the IoV and it refers to the network of dissimilar entities road transport, such as vehicles, foot-travelers, roads, parking lots and city infrastructure and offers real-time communication among them. The IoV is an IoT application that offers a solution for the flow control of traffic and secure communication in cities based on the technology [3]. The increment of the vehicle connectivity to IoT results in the formation of the IoV network. This is a developing field for the automotive industries and one of the significant aspects of the smart cities which helps to monitor the traffic. It is a scattered network that provisions the usage of data formed by linked vehicles and VANETs [4]. The increase in the people drives vehicles results in the corresponding increment of the fatality which occurs because of accidents. A significant objective of the IoV is to permit vehicles to communicate in real-time with their human drivers, foot-travelers, other vehicles, roadside set-up and fleet supervising systems[5]. The IoV supports different types of communication within the network as Vehicle-vehicle (V2V), Vehicle-sensors (V2S), Vehicle-infrastructure (V2I), Vehicle-road side (V2R), Vehicle-cloud (V2C), Vehicle-network (V2N), Vehicle-pedestrian (V2P), Vehicle-devices (V2D) communication. V2V wireless communication is the transfer of information regarding the position and speed of the surrounding vehicle. V2S technology enables sensor communication with neighbor vehicles using pre-installed On-Board Units (OBUs). The V2I is used as an IoT sensor to monitor vehicle internal performance through OBUs. V2R

*Research Scholar, Computer Science and Engineering Department, Chandigarh University, Mohali, Punjab, India, And Assistant Professor, Computer Science and Engineering Department, CGC College of Engineering, Mohali, Punjab, India (kumarsumit.cse@gmail.com).

†Associate Professor, Computer Science and Engineering Department, Chandigarh University, Mohali, Punjab, India (cec.jaspreet@gmail.com).

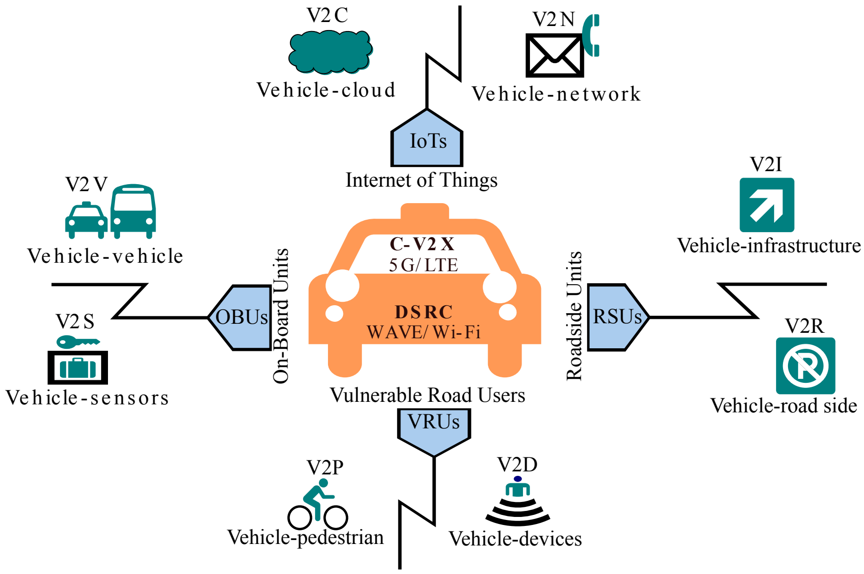

Fig. 1.1. *V2X Communication modes in IoV*

Table 1.1
Analysis of Short-range Communication Technologies in IoV

Parameters	**Bluetooth**	**UWB**	**Zigbee**	**Wi-Fi**
IEEE Specification	802.15.1	802.15.3a	802.15.4	80.2.11 a/b/g
Application	In-vehicle devices connectivity for infotainment	Enable real-time localization with other technologies	Interconnection of sensors with vehicles and RSUs	Enable V2X modes of communication
Domain	Telematics, Body	Telematics, Power train	Body	Telematics
Data-rate	01 Mbps	100 Mbps	250 Kbps	54 Mbps
Range	Up to 10 m	Up to 10 m	10 – 100 m	Up to 100 m
Power Consumption	Low	Ultra-Low	Very Low	High
Modulation Type	GFSK	BPSK, QPSK	BPSK, QPSK	BPSK, QPSK
Frequency Band	2.4 GHz	(3.1 to 10.6) GHz	(868, 915) MHz, 2.4 GHz	(2.4, 5) GHz
Max Bandwidth	Near to 1 Mbps	Near to 100 Mbps	Near to 50 Mbps	Near to 50 Mbps
Protection Techniques	CRC-16 bits	CRC-32 bits	CRC-16 bits	CRC-32 bits
Network Topologies	Spoke-hub	Peer-Peer (P2P)	Spoke-hub, Mesh	Spoke-hub

used to support the wireless exchange of information between a vehicle and supporting Roadside Units (RSUs). V2C and V2N allow the vehicle to access additional information from the cloud and fog server through APIs using the internet. V2P and V2D systems support awareness for Vulnerable Road Users (VRUs) or such as horse riders, pedestrians and cyclists having smart watches or mobile phones. Two or more than two objects communicate in real-time using many diverse technologies which makes IoV complex network. These basic types of communication in ad-hoc networks referred to as Vehicle-everything (V2X) communication that have proposed from a study on [1, 6, 4] in the Fig. 1.1.

V2X communication possible in two different ways, using Wi-Fi technology or 5G/LTE networking for IoT based Internet of Vehicles. The DSRC is responsible for communication between the RSU and the OBU by wireless connection based on WAVE standards. After considering these wireless technologies that used to maintain security and fast communication in the IoV network, some essential communication technologies based on various parameters has summarized in the Table 1.1.

This analysis has done based on work from [7, 8] in which radio technologies are superior to Zigbee and Bluetooth while considering in-vehicle applications depending on low bitrates and inadequate power source and also its low energy ingestion that could offer an extended lifetime. On the contrary, data at fast speeding-vehicle applications could help from the usage of Wi-Fi and Ultra-wideband (UWB) due to their less normalized energy consumption rate.

IoV uses technologies such as navigation systems, mobile communication, and sensor networks for data interchange and instruction systems. Cyber-physical system (CPS) is a combination of cyber (virtual) and physical (real) systems with networking and computation capabilities.

IoT applications typically include three basic layers:

- **Sensor (actuator) layer:** Use to understand (sense) road and traffic conditions.
- **Application (control) layer:** Analysis of data collected by the integration of big data with fog infrastructure in data centers.
- **Communication layer:** Smart wireless connectivity between sensors and fog servers.

In IoT, physical devices are connected over the Internet so that they can communicate with each other and make decisions intelligently and exchange information without or with little human intervention [9], for example, driverless cars or drones.

1.1. Issues and Challenges in IoV. The main focus of the Internet of Vehicles is to connect multiple users with vehicles, devices and networks, offering a safe and secure communication capability that is flexible, efficient and reliable. The construction of IoV with such multiple objects makes it a complex system [10]. Also, the use of IoV is less diverse compared to other networks and as a result, there are some particular requirements. Both of these issues add new technological challenges and test the research and development of IoV. During discussion related to the function and construction of IoV, here are some of the issues and challenges that researchers face:

- **Security and Privacy:** Since IoV combines a wide range of various services and standards, there is a requirement for the safety of information. As an open community network, IoV is aimed at cyber attacks and attacks that can cause physical loss and privacy leaks. Maintaining the balance between privacy and security is one of the key issues in IoV. The acceptance of reliable info from its sender to the recipient is important [11]. However, the senders' privacy requirement may be violated by this reliable information.
- **Vehicles Reliability:** Vehicles, sensors, and network sensors may fail sometime. The system has to deal with inaccurate data, plus malicious communications, for example denial of service (DOS) attacks. Some technologies can be deployed like Intrusion Detection Systems (IDS) to protect against attacks in traditional networks [12]. In general, car safety is very important compared to in-car entertainment.
- **Mobility and Dynamic Topology:** Compared to other vehicles in the network, cars can travel at much higher speeds, resulting in constantly changing network topologies. It requires a test to connect with consecutive nodes and transport the goods from one place to another. Therefore, the flexibility of network topology should be considered important for IoV development.
- **Open Standards:** The absence of standard can make successful V2X communication troublesome, so interoperability and standardization are required for quick selection. Receiving open standards will empower the flat-sharing of data. Governments ought to take an interest and urge enterprises to work together in the improvement of innovative prescribed procedures and open global standards.
- **Variable network load:** Network size is another big challenge, which can be very high or low due to changing traffic conditions. As the scale of the network in large urban areas can be high, for example, entries in urban areas, main highways, and metropolitan cities. In any case, if the network has severely broken can now remain fragmented, which cause road accidents. Therefore, a smart traffic surveillance system based on 5G technology will be required to solve this problem [13].
- **Geographical Communication:** Related to different networks that use multicast or unicast routing, where communication is reflected by a particular ID, car networks often have some form of transmission, which affects areas where bulk traffic should be sent.
- **Predictable Mobility:**Vehicular networks are different than different types of specially designated networks where nodes move randomly. Cars, in turn, are forced by topology and design, by the need to pay attention to traffic signals and traffic signals, and by the reaction of moving neighbour vehicles, which makes consistency as far as possible.
- **Sufficient Energy and Storage:** The general feature of nodes in Vehicular networks is that they contain more power to register (count, maintain and adjust), because nodes are in rows rather than

smaller portable gadgets.

- **Various Communication Environments:** Vehicular networks have generally used in two common communication areas. First, in the case of highways, the situation is generally basic and direct. In the case of cities, this has really problematic because the routes have isolated by divisions, such as sectors, trees, and other different obstacles [14].
- **Poor Network Connectivity:** As high mobility of devices and fast changes of network topology, leading to network partitioning and connection disappointment result in bad messages should be normal. At that time, the need for ways to joining back to the network is always being explored.
- **Hard Delay Constraints:** In IoV, many applications have severe delays, even they do not require high-bitrate or bandwidth. Such as, during a serious incident, a message must be transmitted and displayed at a specific time to avoid a car accident. Current application, instead of the usual delay, undesirable delays will be important.
- **Big data in IoT:** One of the biggest challenges is the processing then storing of the large amount of data generated in the IoV due to a high number of connected autonomous vehicles, which has assumed to be 1Gb per second of data processing [15]. Therefore, it is a vital function for big data management in intelligent connected vehicles (ICV) using cloud computing and IoT analytics.
- **High-Reliability requirement:** Transportation-related applications are often very delicate, so there is a requirement for high-reliability. Since complex systems, network-level size, and poor power of connectivity, high-reliability in IoV is difficult to achieve.
- **Service Sustainability:** Ensuring the robustness of service delivery in IoV is still difficult as it is, it calls for high-level perceptual strategies, just as it is not easy to understand the network system. There is difficulty in adapting all vehicles to provide sensible types of assistance with amazing networks gradually, as it is necessary to have network bandwidth, remote access, low service levels and host status.

These security and trust-related issues of IoV are expected to be resolved in the future to make it more reliable and successful.

1.2. Applications. Most of the IoV applications are in the field of telecom. According to Cyber-physical systems (CPS) some important applications of the IoV model and their functionality are classified into different classes, given below:

- *Safety:* Cooperative collision avoidance, Lane changing warnings, automatic braking and speed control
- *Navigation:* Real-time traffic, Route navigation, Locating parked vehicle, Cooperative driving
- *Information and Infotainment:* Wi-Fi in vehicles for downloading of music, video streaming, content sharing
- *Remote Telemetric:* Vehicle remote locking, Car surveillance
- *Diagnostic:* Service spot detection, Self-repair, Fuel usage optimization
- *Car sharing:* Car pooling, Group parking booking
- *Others:* Electronic toll payments, Traffic flow monitoring, etc.

The Internet of things and Cyber-physical systems are not isolated technologies [16]. Cyber-physical systems (CPS) and IoT in the IoV network have some other important applications, such as Intelligent transportation systems (ITS), Connected autonomous vehicles (CAV), Smart grid, Smart city, and Smart manufacturing [17].

1.3. Motivation. In the upcoming time, IoV will become the future of the VANETs based on the expansion of the web services. An essential portion of the Internet of Vehicles having different exploration fields, including intelligent transportation system, wireless communication, cloud and fog computing, mobile computing, autopilot vehicles and era of CPS [18]. On the routing and packet data transmission point of view, both network security and robust data transmission are necessary for different applications. IoV networks mostly consist of vehicles, which operate in a very different way than wireless sensors. As a result, the IoV network has many features that can influence the formation of IoV technologies. Some features will present difficulties for the advancement of technology, and some may result in benefits.

1.4. Contributions. Motivated by existing problems in IoV, we present a new approach for improved traffic management and reliable communication in IoV using behavioral studies of IoT and VANETs. The significant contribution of our work lies in summary as follows:

- In this paper, we have proposed and designed a novel framework (CSI model) for IoV with studies based on the current VANET environment to prevent traffic congestion, maintain secure communication, and maximize data delivery.
- The purpose of this study is to analyze various mechanisms for better route selection based on vehicle range, residual energy, and vehicle condition for efficient communication using artificial intelligence.
- The future challenges and current issues for the design and development of IoV networks with the help of big data, IoT, and cloud services have discussed in detail.
- This paper sheds new light on the full layered architecture of IoV for a better analysis of existing models.
- This survey presented various communication strategies for IoV by reviewing existing routing protocols, topologies, and applications.
- In conclusion, comparisons have made for the performance of existing works in terms of Quality of Service (QoS) parameters to explore better possibilities towards faster and reliable data transmission in IoV networks.

1.5. Organization. This paper has divided into five sections. Section 1 gives a brief overview of the IoV network with current issues, challenges, applications, and motivation for contributions. The rest of this paper is structured as follows. Section 2 describes an in-depth background survey explaining their respective approaches, limitations, findings, and future research gaps. Section 3 presents the layered architecture of the IoV with its routing protocols and security requirements. The performance of existing works has evaluated and a proposed novel framework presented in Section 4. The paper concludes with future scope in Section 5.

2. Background Survey. The survey of existing work for the secure communication and traffic congestion minimization in IoV is discussed in this section of the paper.

In 2019, Muhammad Asim Saleem et al [1] has researched information transmission using IoT based VANETs with congestion control mechanisms and the key highlights are listed as:

- Researchers has used the concept of basic routing protocol standards for VANETs. The proposed routing mechanism requires a large amount of energy used to consider routed between vehicles or RSUs one after another.
- Here center of attention is to intend a multiple mediator system for completing the route discovery mechanism in VANETs. Designing routing mechanism is grounded upon four mediators (intermediate communication vehicles or RSUs), which are coordinated in finding ideal paths and in reducing the traffic congestion inside the network.
- Therefore, an efficient hybrid clustering based routing mechanism is a better option for data packet transfer with IoT based VANETs to reduce traffic interruption.

In 2018, Lucy Sumi and Virender Ranga [2] designed an IoT based VANET for the controlling the traffic to help emergency vehicles in a smart urban city and some of the observed conclusions are written as follows:

- The authors introduced a structure of merged concepts from IoT and VANET that target the easy passage for precedent emergency vehicles via the traffic path, and this traffic congestion is a big issue.
- The suggested system helps the emergency vehicles and ambulances in searching the adjacent feasible route to their destination based upon the real-time traffic data.
- The proposed system supports reducing the delay in transmission time for any medical help during mishaps and the timely delivery of medicines to patients.

In 2019, Amr Tolba [3] has presented a content accessibility preference approach for improving service-optimality in IoV; the key highlights are listed as:

- The author has given a technique of obtaining data at low-delay to enhance the service-optimality of smart vehicular applications.
- By taking optimal gateways, the vehicles for getting access to data use the advantages of epidemic spread routing.

- The author has designed a content accessibility preference (CAP) prototype that helps in accurate vehicle selection.
- The effectiveness of the suggested CAP design is validated using various QoS parameters such as throughput, packet transfer or service rate, vehicle service ratio, and delay.

In 2017, Zhenyu Zhou et al. [4] presented big data-based data propagation in VANET and the key highlights are listed as:

- The authors have examined the content propagation difficulty in IoV networks based on D2D and V2V communication.
- The physical, as well as social layer data in the context of link possibility as well as social association rigidity functioning to resolve the framed combined power control, peer discovery, and channel selection problem.
- The projected scheme was associated with two experiential processes, and its efficiency and power in the sum rate, as well as content approval, were authenticated using results.

In 2017, Zhaolong Ning et al. [5] projected a cooperative QoS access scheme for Social-IoV (S-IoV) and below is some relevant points relating to this research:

- Firstly, the authors studied an active access service assessment scheme to manage through the consequence carried by the dynamic network alteration. They construct a CQS access system, concentrating on consistency assurance and service excellence promotion in Social IoVs.
- Secondly, the paper offered a social association assessment technique for exploring internal as well as external similarities between vehicles. Additionally, they examined a forecast technique consistent with the vehicle movement path for communication time valuation.
- In the end, they presented a CQS technique, which initially constructed a node-centric formation of hierarchy and arrangement to calculate the contact excellence, and then selects a contact path based upon the existing state of the network. Also, the bi-direction buffering procedure is inspected to enhance the response competence as well as procedure accuracy.

In 2016, Jiafu Wanet al. [6] projected mobile crowd-sensing for traffic forecasts in IoV and the observed conclusions are written as follows:

- Originally from the perspective of service relationships between fog computing and IoV, the authors have talked about the classification of cloud or fog-based Internet of vehicles.
- Authors have projected mobile crowd-sensing for traffic forecasts on the Internet of Vehicles (IoV).

In 2017, Wenchao Xu et al. [19] plotted the Internet of Vehicles (IoV) in a Big Data era to analyze relationships between them and some of the observed conclusions are written as follows:

- The authors highlighted and extended the significant role of the IoV using big data for autonomous vehicles.
- In addition, they identified emerging problems in IoV to demonstrate several required guidelines for the future Internet of vehicles (IoV) in a big data period.

In 2018, Xiaojie Wang et al. [20] offered a reasonable solution that allows off-loading for real-time traffic organization in Edge-based Internet of vehicle (IoV), to reduce the system average execution time. The key points related to this study are as follows:

- Firstly, offered a reasonable solution, which allows for off-loading real-time traffic organization in Edge-based Internet of Vehicles (IoV) to reduce the average execution time of the system.
- The authors have not investigated how to use external vehicles from a range of roadside-units (RSUs) communication to offload the data from fog nodes for traffic management systems (TMS).

In 2016, Jiawen Kang et al. [21] purposed two computer-generated mechanisms for plotting outbreaks and safeguarding for IoV. And the key highlights are listed as:

- Firstly, present the IoV prototype and then designate location concealment and plotting by two representative virtual machines.
- In an active topology, the communication rules in a secrecy protection order among local or in-house clouds setup and vehicles should be secure and effective to reduce the usage of the framework.

In 2017, Jiawen Kang et al. [22] presented privacy-preserved pseudonym plan for Edge computing-based IoV network. And below are some relevant points relating to this research:

- They introduced path info secrecy issues on the Internet of Vehicles with a new model called Fog or Edge-based Internet of Vehicles (F-IOV) for successful pseudonym organization using devices on the fog layer.
- Pseudonyms are created and spread to automobiles with time for safe communication and privacy management in IoV.
- Their proposed system is not much valid for conditions related to light vehicles, also does not study social networks.

In 2016, Eun-Kyu Lee et al. [23] presented the IoV from a smart grid to self-directed fog or edge-based vehicles. And the key highlights are listed as:

- This editorial appealed that the vehicular cloud model which is equal to Internet-based cloud structure for vehicles, would be the essential framework surrounding that creates the progress probable and that the self-directed manipulating would be the main recipient in the cloud planning.
- The authors introduced a vehicle cloud model for future research, which emphasizes the use of unmanned aerial vehicles (UAVs) and also explained the future research approaches.

In 2017, Wenyu Zhang et al. [24] purposed a model of cooperative fog computing amid Big Data on the Internet of Vehicles. And below are some relevant points relating to this research:

- They presented difficulties with cloud-based IoV networks, and planned a local IoV design for low-delay communication services.
- They discussed resource management scheme for this improvement in IoV designed, including intra-edge power-efficient and inter-age QoS-efficient resource management.
- Further, they provided the necessary simulation outcomes to prove the efficiency of the model employed.

In 2015, Anand Paul et al. [25] purposed a helpful perceptive intellect for the internet of vehicles. And some of the observed conclusions are written as follows:

- There are conflicts among better vehicular communication and high wireless mobility with a deficiency of computational resources and low bandwidth.
- Therefore it requires an inventive Cognitive Radio (CR) and effective spectrum management as well.
- The projected scheme utilized to reduce both high vehicular mobility as well as the spectrum deficiency problems.

In 2018, Priyan Kumar et al. [26] offered an active traffic management plan with the help of the Internet of Vehicles for optimal route selection. And the key highlights are listed as:

- The road map presented here is further divided into small numbers of groups. In addition, the ant colony optimization (ACO) algorithm is used on these maps to find the best routes.
- Additionally, they have proposed a fuzzy logic function for estimating huge traffic capacity and designing.

2.1. Research Gaps. After careful analysis of the literature survey and findings discussed above, various solutions have been found for smart and secure communication, which provides better results in reducing traffic congestion. And the following main highlights are as follows:

- It can be deduced from the above existing works that, routing is used the concept of intermediate vehicles is a time-consuming process. A clustering-based routing mechanism would be a better solution to achieve the maximum data delivery ratio [1].
- Researchers have proposed various routing mechanisms such as proactive, reactive, hierarchical, and hybrid to prevent traffic congestion in VANETs. In such cases, both normal messages, as well as emergency messages, sent with the same delay in transmission [2].
- The existing mechanism for IoT-based VANET uses a general algorithmic framework that needs to be updated with the concept of Artificial intelligence and optimization to minimize delay in transmission [3, 4].
- IoT is one of the most emerging and innovative areas that need to be implemented in VANETs or existing ad hoc networks for secure communication, accident prevention, and traffic management [6, 5].
- A challenging area in the field of IoT based VANET is network protection from various attacks and secure communication, not found in existing works [21].
- The present VANET has a low data delivery rate due to the complex interaction between human

Table 2.1
Survey of Related Work

Year	Author/s	Proposed Work and Approach	Limitations
2019	Muhammad Asim Saleem et al. [1]	Data transmission using IoT based VANETs with congestion control mechanisms. Approach: MAC protocol with mediator selection method.	The expected routing mechanisms in practice comprise a large network field, where the mechanisms required a large amount of energy to visit one by one vehicle/RSU en-route. Hence, an effective hybrid clustering based routing mechanism for packets information transfer utilizing IoT driven VANETs to reduce vehicular congestion is a better option.
2018	Lucy Sumi and Virender Ranga [2]	Designed an IoT based VANET used for traffic controlling structure in a smart city for emergency vehicles. Approach: IoT based VANET.	Authors do not consider a secure reliable routing mechanism for controlling traffic influenced by attacks or intentional obstruction, which itself is exceptional and should be studied.
2019	Amr Tolba [3]	Content accessibility preference (CAP) approach for improving service optimality in internet of vehicles. Approach: CAP model with Epidemic spread routing (ESR).	The author has suggested a technique of obtaining data at low delay to enhance the service optimality of smart vehicular applications. By choosing optimal gateways, the vehicles for getting access to data exploit the advantages of ESR.
2016	Zhenyu Zhou et al. [4]	Presented dissemination of social Big Data information in IoV. Approach: Hybrid V2V-D2D driven Internet of Vehicles.	The experimental results of this designed network show that the system efficiency is increased by utilizing the hybrid approach, but the routing overhead problems of the network are not solved in case of a large number of vehicles.
2016	Z Ning et al. [5]	Proposed a co-operative quality-aware, S-IoV access service model. Approach: SIoV and co-operative Quality Aware Service Access Structure (CQS) model.	The work has been conducted assuming a network of fixed number of vehicles. In the case of new vehicles, which want to join the network during the simulation, the achieved system performance is degraded for high bandwidth requirements.
2017	Jiafu Wanet et al. [6]	Mobile crowdsensing for traffic prediction in IoV. Approach: IoT, data aggregation method, cloud computing.	The proposed model overcomes the deficiency of the existing model by using the data aggregation in case of less communicating devices, although for a large amount of communicating devices the rate of data transmission is reduced.

behavior and vehicles. As driving behavior shows the influence on human decisions, intelligent vehicles can not only act as human, but also make decisions according to requirements [22, 23].

The main issues not considered in the existing works are secure communication and network security, after which vehicle traffic congestion is another major problem for any developed or developing country. With the increment in the number of connected cars, a huge amount of data plus traffic also expected [27]. Due to traffic congestion a lot of inconveniences such as road accidents, the amount of fuel consumed by vehicles is large, air and sound pollution, damage to the vehicles occur. To analyzing precise traffic congestion control mechanisms are very much required to provide efficient and sophisticated functioning of a network with security. Web of things (IoT) helping the transformation of conventional VANETs into the intelligent vehicular ad-hoc networks (InVANETs) for Device-device (D2D) communication [28]. This helps improve road safety and efficiency of the VANETs by adopting a cluster-based routing scheme. The most important goal of any IoV model is to transmit the data packets within a network with maximum delivery rate and to achieve this task, IoT based communication is the best solution that can be observed by analysis of Table 2.1.

Table 2.1 represents an analysis of existing work based on the approaches used and their limitations, and the findings of existing research have described in Table 2.2 below with the work proposed by the authors.

IoV depends on VANET, so it needs more analysis on VANETs based on its routing protocols, artificial intelligence, and optimization techniques. VANET is the resultant term originated from the general word "Ad-Hoc Networks". VANET is a subcategory of Mobile Ad-Hoc Network (MANET), and VANETs also face many challenges that are common with MANETs [36]. Due to the development in vehicle industries, wireless communication and telecommunication results to the advancement in VANET. In this network, vehicles are taken as nodes that are movable and sharing the information between the nodes for creating a network. Vehicles that are under the field of another node, may communicate with that node plus turn out to be as a part of the network. There are mainly three kind of connection feasible in vehicular ad-hoc networks called Vehicle-vehicle (V2V), Vehicle-road side units (V2R) plus clustering based routing protocols. Several IT and vehicle industries are operating collectively for organizing VANET and offering protection to consumer, consistent data

Table 2.2
Findings from Related Work

Year	Author/s	Proposed Work	Findings
2019	Elgarej Mouhcine et al. [29]	A smart routing scheme in VANET using a distributed Ant Colony Optimization (ACO) was projected.	The projected scheme relies on the VANET architecture and is followed by a dispersed ant system (DAS) algorithm. DAS is an example of swarm intelligence, which provides good results for searching the shortest and finest routes. The results showed that the technology not only reduces traffic congestion by rerouting vehicles, but also helps reduce overall waiting time.
2019	Christy Jackson Joshua et al. [30]	A multi-objective firefly optimization approach (FOA) dependent weighted clustering routing protocol in VANET was designed.	The authors discussed the difficulties of clustering in a reliable weighted clustering routing protocol with the Firefly-optimization algorithm. The results differ from other related methods such as Comprehensive Learning Particle Self Adaptation (CLPSO) and Multi- objective PSO with a summary obtained from Chennai (Urban) in India. A similar form of the evolutionary algorithm used for Multi-objective with the help of multiple processors to increase performance with reduced computational time.
2019	Mrigali Gupta et al. [31]	Designed a Particle Swarm Angular Routing for Vehicular ad-hoc networks (PSARV).	The authors suggested an active particle swarm angular routing protocol for VANETs (PSARV) that applies the PSO technique as angular routing to search an appropriate route. The RREQ-swarms routing executes more proficiently than the DSR considering throughput and packet loss. The predicted process can be applied to a swarm leader who depends on swarm multi-casting for the safety of passengers. Therefore, all the vehicles in this path are informed about hazardous situations onward, so that they are alert and aware in advance. The future goal is to estimate the performance of PSARV network scenarios in live traffic.
2019	Xi Hu et al. [32]	Proposed a model for VANETs using the concept of social co-operative driven vehicle-to-vehicle broadcasting optimization algorithm.	Proposed V2V broadcasting optimization algorithm based on social coalitions. Simulation results prove that the SCBO algorithm not only keeps the highest possible rate under varying node densities, but also increases the transmission saving rate to reduce the average end-to-end delay time.
2018	Jamal T. and Enrique A. [33]	Designed a vehicular network based on swarm intelligence algorithm for collaborative traffic.	Swarm FREDY advised a Swarm Intelligence inspired scheme for congestion control in VANET. FREDY has shown greater stability and more options for advancement than DIFRA. Since the beacon rates calculated through the first technique are often lower than those calculated by Swarm DIFRA.
2017	Ramesh C. Poonia [34]	Discussed the routing protocols for VANETs with swarm intelligence for performance evaluation of the network.	This article presented a VANET based on swarm intelligence and also examined the QoS of some routing protocols based on swarm intelligence like Time-ant, ACO-RA, Hy-BR, PRA, and Bee-Ad-hoc. They conclude Bee-Ad-hoc and Hy-BR is the most suitable routing algorithm in VANET but the network security is poor and will be improved by applying artificial intelligence techniques with swarm intelligence technology in the future.
2019	R. Yarinezhad and A. Sarabi [35]	Projected a new routing algorithm for VANETs driven Glowworm Swarm Optimization (GSO) algorithm.	Using GSO, the proposed algorithm detects optimal routes between 3-way congestion with intersections, and packets are delivered based on optimal routes, which are also fit for congested situations. Simulation results show that the designed algorithm is better than GSO and another two algorithms OSTD and SAMQ. Furthermore The GSO algorithm requires a large number of glowworms to build an optimal path and need artificial intelligence for better results.

interchange and providing the optimal path. One of the main tasks in VANET is to discover the optimal path or to find the target's node position. Varied researchers are trying their hand in this area for optimizing the route or searching the destination in VANET in a consistent manner. Numbers of optimization procedures are existing being encouraged from nature and also has own varied characteristics and calculates diverse method for solving problems and for optimization of the results.

After the survey, the next section discusses the layered architecture of IoV, which helps explore the characteristics and challenges of smart and secure communication for better understanding.

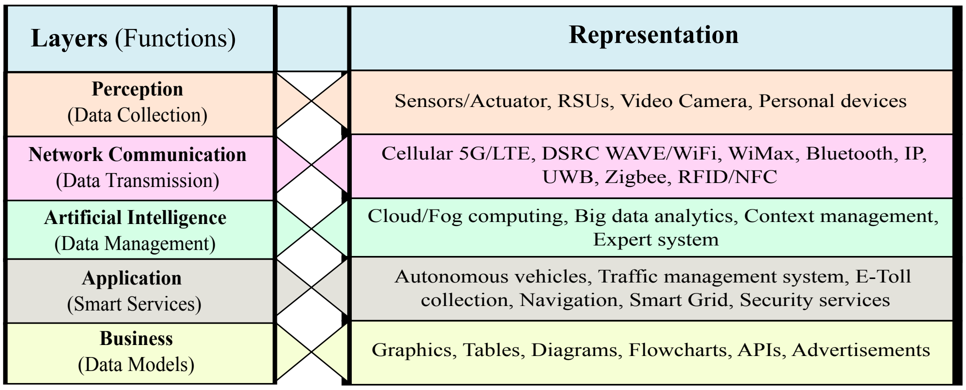

Fig. 3.1. *IoV 5 layers architecture*

3. Layered Architecture and Protocols. Layered architecture design of complex networks such as IoV with various technologies is a challenging task that needs to identify and effectively group a set of elements with similar functionality and representation. Several researchers have proposed different layered IoV architectures.

3.1. Layered Architecture. A five-layered architecture is depicted in this section, which includes perception, network, artificial intelligence, application, and business layer. The functionality and representation of each layer have briefly described below, with the proposed Fig. 3.1 from studies on [37, 38] has the typical IoV architecture.

- **Perception Layer:** Perception layer includes each sensor inside the vehicle that collects natural data to make precise decisions for various driving patterns and traffic conditions use, such as satellite sightings, road traffic monitoring, vehicle position recognition, and vehicle monitoring.
- **Network Layer:** This layer establishes communication using heterogeneous networks like Cellular 5G/LTE, DSRC WAVE/Wi-Fi, WiMax, GSM, WLAN, Bluetooth, Radio frequency identification (RFID) signals and many other modes of wireless communication for Vehicle-everything (V2X) modes.
- **Artificial Intelligence Layer:** It is the heart of the IoV model which is used for computing, processing and storing of the information. This layer having sub-layers like sensing, data mining, analytics and intelligent control layer.
- **Application Layer:** This layer contains statistical tools, storage provision, and infrastructure operations that are responsible for analysis, processing, storage, and decision making for risk factors like traffic collisions, bad weather. Here smart real-time apps, traffic safety, efficiency, and multimedia data used.
- **Business Layer:** This layer contains operational and management logic related to the business aspect, mainly for the development of business models and statistical analysis of the vehicular data. For these tasks, various analysis tools use, such as flowcharts, graphs, tables, diagrams, and use cases.

3.2. Routing Protocols. As high flow in the vehicle network, the most difficult task is data routing or connection establishment process. There are five categories of routing protocols in the Internet of Vehicles (IoV) model, which are listed and discussed below with the help of diagram 3.2:

- **Position or Geographic Based (Unicast):** These routing protocols consist of a variety of algorithms for exchange details about the geographical positioning to pick the next forwarding nodes. The information is communicated to the one-node neighbour, which is nearest to the target, without any route information. So, this routing method is useful, as there is no requirement to build and maintain a universal route from source to target node like location-aware routing for Unmanned Aerial Vehicles in software-defined networks [41]. The rank based route is mainly divided into two classes: Location-based greedy Vehicle-vehicle networking and Delay-Tolerant Networking (DTN) Protocols.
- **Topology Based:** These protocols use the details links available on the channels for data packets delivery. These are mainly separated by Proactive, Reactive and Hybrid types. Proactive is table-

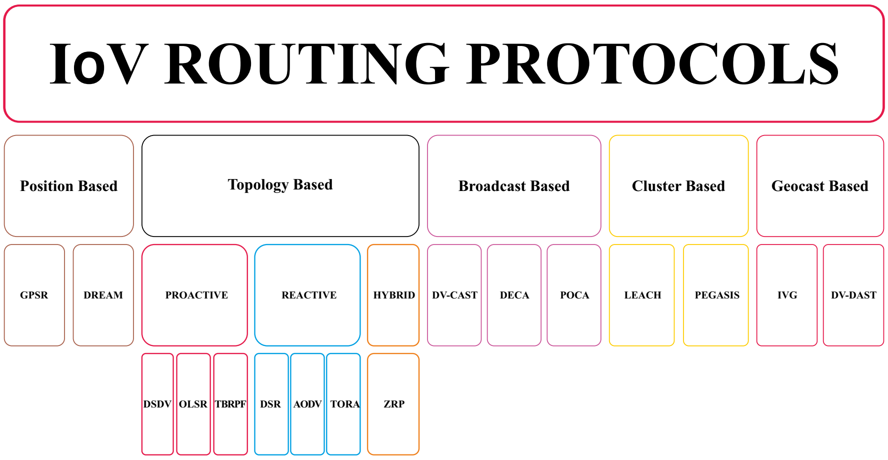

FIG. 3.2. *IoV Routing protocols taxonomy adapted from [39, 40]*

based routing, where every hop maintains a routing table. Reactive is on-demand routing, there is no need to maintain the routing table. Hybrid routing is a combination of both, where the network is divided into zones [42].

- **Broadcast Based:** Broadcast based routing is widely used in the vehicular network for data sharing regarding weather, emergency and traffic conditions between vehicles as well as delivery of advertisements and announcements.
- **Cluster Based (Multicast):** A collection of hops describes itself as part of a cluster from which a hop is selected as the cluster head (CH) to distribute the packets. Cluster head (CH) selected based on specific selection criteria. Scalability can be given in large networks, but delays will be found when grouping in most vehicle networks. To implement scalability, a virtual network structure needs to form by the clustering (grouping of hops).
- **Geocast Based (Multicast):** The Geocast route is a multicast-based geographic location [43]. Its purpose is to pass the packet from single-vehicle through multiple vehicles to reach the destination based on their local geographic region known as Zone. Unicast routing may be applied to deliver the packet inside the target zone. In Geocast, vehicles outside the simulation area are not warned to bypass the unwanted extra-fast response. One disadvantage of Geo Cast is network segmentation, as well as the next adverse nodes, which can interrupt the usual information delivery.

Nowadays, VANETs integrate with software-defined networking (SDN), which requires a more flexible content-centric networking approach as opposed to multicasting [44]. Whereas active assemblies of basic VANETs should be used for a unicast message communication at present; as there are still many applications that require seamless unicast routing.

3.3. Security requirements. The above survey concluded some basic security requirements to protect the vehicle network from attackers and maintain secure communications, listed in the following Table 3.1: The layered architecture, routing protocols, and security requirements have discussed in this section, but the use of intelligence needs to be explored more with the help of a new proposed model. Therefore, to analyze the impact of artificial intelligence and machine learning, some important conclusions have proposed in the following section.

4. Analysis and Proposed Framework. In this part, the existing works have analyzed using QoS parameters like throughput and packet loss for comparing and observing values from the simulation section of [1, 2, 3, 4] in terms of throughput and packet loss. Throughput typically represents an average feasible or the transfer rate between two nodes. Throughput is usually inversely correlated with the possibility of packet loss, as packet loss leads to a slow throughput rate. Therefore, to compare and analyze existing works, calculated the average Throughput based on unit conversion (like Kbps to Mbps or Gbps to Mbps) and Packet Loss

Table 3.1
Security requirements in VANET based on[45]

Parameters	Description
Non-Repudiation	This avoids frauds from denying their offenses because in this case even if the attack happens, unrepentant will expedite the capability to detect attackers.
Availability	Vehicular networks will require real-time for many purposes and should therefore always be available. These apps require high speed from sensory networks or through the Ad-hoc network, the resultant elimination may be or the massage can be a little useless if there is a hold of seconds in various applications.
Confidentiality	This security requirement assured that information will be read by allowed users only. A need for confidentiality is required in group communications, where team members are not allowed to read such information.
Authentication	It assures that the data has been entered by an authentic user. The data accessing the physical stream must be precise and established by the authentic person because in IoV, the reaction nodes according to data established from the other end.
Integrity	It ensures that the data in the sender and the sender side are the same Message conversion is done by authorized users only. The recipient uses the same process as the one used on the sender's side to create the second call from the message comparing it to the first message. This process ensures the integrity of the data.

Table 4.1
QoS Parameters Comparison

S.no	Authors	Average Throughput (Mbps)	Packet Loss Rate (%)
1	**Muhammad Asim Saleem et al.** [1]	5.30	12.77
2	**Lucy Sumi and Virender Ranga** [2]	53.94	23.74
3	**Amr Tolba** [3]	95.17	9.83
4	**Zhenyu Zhou et al.** [4]	85.33	8.87

(Sometimes known as Total packet/Success transfer rate). In these research articles, simulation parameters have calculated with different scenarios, and comparisons between them are not possible depending on the scenarios considered. Analysis based on QoS parameters, such as throughput and packet loss, is shown in the Table 4.1 to compare existing work; their graphical representation is in Fig. 4.1.

Table 4.1 and Fig. 4.1 represent a comparative analysis of the IoV model in previous years proposed by various techniques and algorithms based on the QoS parameters. Fig. 4.1 (a) represents the comparative analysis of observed throughput in different scenario for IoV, but in case of work proposed by [3] and [4] is much better compare to the others because they use the concept of estimation of headway distance of vehicles as a Wiener process by exploiting Kolmogorov equation to maintain the connectivity of the vehicle. The transmission loss of existing work is represented in Fig. 4.1 (b) with comparative analysis in different scenarios for IoV and the transmission loss of work proposed by [3] and [4] is less due to stable connectivity between the vehicles. From the Fig. 4.1, some observations have shown that the models designed by different researchers have their advantages and disadvantages, but the use of artificial intelligence is a beneficial step for secure communication in IoV networks with existing works.
Additional studies are required to build a smart and reliable IoT based VANET model using artificial intelligence techniques.

4.1. Proposed Framework. Based on the above survey findings and gaps analysis, IoT-based VANET and intelligent services have used to design a proposed Cluster-based, Self-organized, and Intelligent (CSI) framework that helps in smart and secure communication thereby reducing traffic congestion, as shown in Fig. 4.2.

- **IoV Setup Phase:** Design and deploy IoT based VANET
  Step 1: IoT has helped develop the ad-hoc network of traditional vehicles into ad-hoc networks of intelligent vehicles.
- **Cluster Setup Phase:** Clusters formation and Data transmission
  Step 2, 3: Define the coverage area for each vehicle/RSU node, which helps to build the route from the source node to the destination node. To solve this problem the selection of Cluster Head (CH) node is

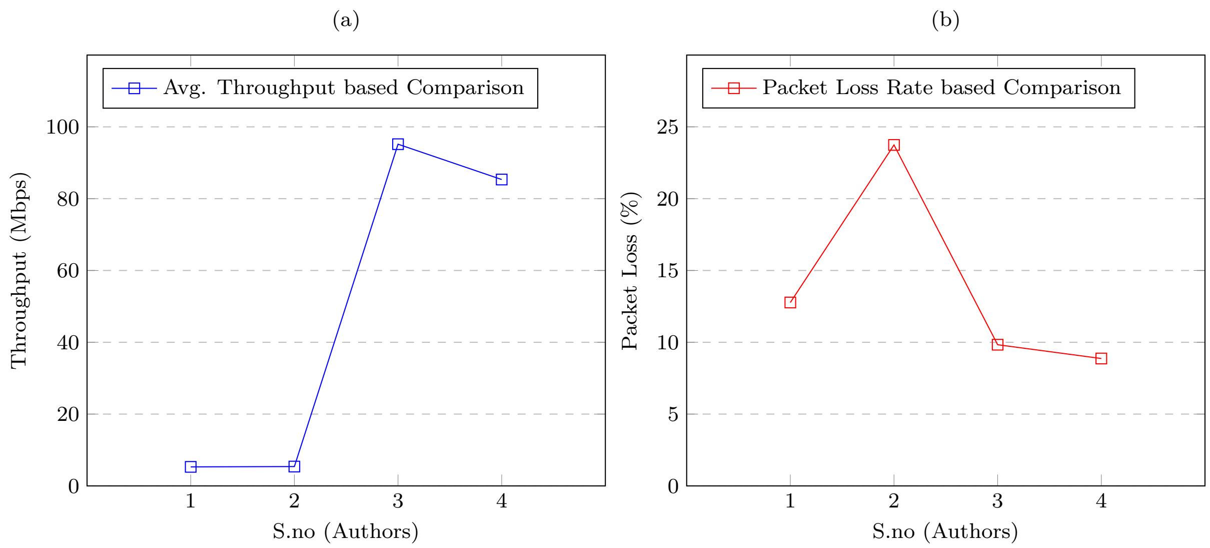

FIG. 4.1. *Comparison of QoS Parameters: (a) Average Throughput and (b) Packet Loss Rate*

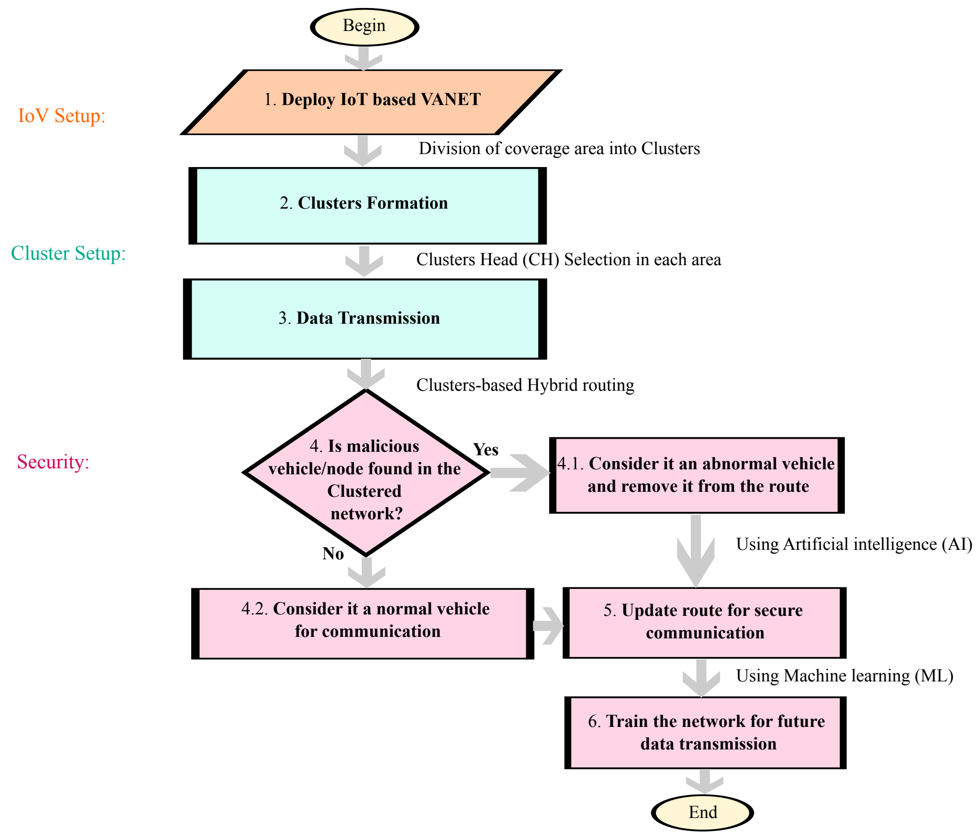

FIG. 4.2. *Proposed Cluster-based Self-organized Intelligent (CSI) Framework*

best suited for better data transmission.

- **Security Mechanism:** Malicious node, Update route, and Network training
  Step 4, 5, 6: When the performance of the network degraded, then the concept of Artificial intelligence (AI) is used to detect malicious or fail nodes in the network, which has not able to communicate with other vehicles/RSU thereby create traffic congestion. The machine learning (ML) algorithm acts as a processing unit that updates itself with changes in routes used for future data transmission.

Some important outcomes based on the proposed CSI model have listed below that will help solve real-life problems in existing IoV networks:

- The use of clustering-based routing approaches with trust management mechanisms will be beneficial for the future internet of vehicles.
- The integration of artificial intelligence with routing mechanisms helps to detect networks blocked by malicious or dead nodes.
- The concept of traffic congestion minimization will be introduced with the IoV network to provide a fast and robust communication.

Moreover, we have decided to use a robust cluster-based routing to validate the proposed work. Hence, future studies on the current topic are required to compare and verify the proposed and existing models based on parameters such as Throughput, Packet loss, Packet delivery ratio, and delay.

5. Conclusion and Future Scope. New communication technologies for vehicles grow mainly from the improvement of basic communication between Vehicle-vehicle and Vehicle-infrastructure, and Vehicle-network. IoV model is a reality at present which is acquired by interconnections of vehicles and traffic infrastructure including people. This paper presented a detailed overview of the IoV architecture along with its routing protocols, issues, and challenges, which helps to build secure communication. IoV network designing is still at an early stage of development, and requires many technical issues to be resolved before it is recognized globally and deployed in modern networks. With the fast growth of computing and wireless transmission techniques, the Internet of Vehicles network offers large business and research importance for security and fast communication. Therefore, in the future, the IoV network is a better option with the concept of Artificial intelligence and Machine learning technology acting as a classifier used to train IoV networks with a reliable routing mechanism based on hybridization and meta-heuristic optimization algorithms adopted for security and fast communication purposes.

REFERENCES

[1] M. A. Saleem, Z. Shijie, and A. Sharif, Data transmission using iot in vehicular ad-hoc networks in smart city congestion," *Mobile Networks and Applications*, vol. 24, no. 1, pp. 248–258, 2019.

[2] L. Sumi and V. Ranga, An iot-vanet-based traffic management system for emergency vehicles in a smart city," in *Recent Findings in Intelligent Computing Techniques.* Springer, 2018, pp. 23–31.

[3] A. Tolba, Content accessibility preference approach for improving service optimality in internet of vehicles," *Computer Networks*, vol. 152, pp. 78–86, 2019.

[4] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, Social big-data-based content dissemination in internet of vehicles," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 2, pp. 768–777, 2017.

[5] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, and M. S. Obaidat, A cooperative quality-aware service access system for social internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2506–2517, 2017.

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

[7] A. Azman, S. Yogarayan, S. L. W. Jian, S. F. A. Razak, K. J. Raman, M. F. A. Abdullah, S. Z. Ibrahim, A. H. M. Amin, and K. S. Muthu, Comprehensive study of wireless communication technologies for vehicular communication," in *2018 3rd International Conference on Computer and Communication Systems (ICCCS).* IEEE, 2018, pp. 314–317.

[8] M. A. Haque and M. D. Hossain, Technology survey of wireless communication for in-vehicle applications," in *The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014).* IEEE, 2014, pp. 1–7.

[9] A. Nayyar, B.-L. Nguyen, and N. G. Nguyen, The internet of drone things (iodt): Future envision of smart drones," in *First International Conference on Sustainable Technologies for Computational Intelligence.* Springer, 2020, pp. 563–580.

[10] J. Chen, H. Zhou, N. Zhang, W. Xu, Q. Yu, L. Gui, and X. Shen, Service-oriented dynamic connection management for software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2826–2837, 2017.

[11] M. Sookhak, F. R. Yu, and H. Tang, Secure data sharing for vehicular ad-hoc networks using cloud computing," in *Ad Hoc Networks.* Springer, 2017, pp. 306–315.
[12] S. Sharma and A. Kaul, A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud," *Vehicular Communications*, vol. 12, pp. 138–164, 2018.
[13] N. A. Khan, N. Jhanjhi, S. N. Brohi, R. S. A. Usmani, and A. Nayyar, Smart traffic monitoring system using unmanned aerial vehicles (uavs)," *Computer Communications*, 2020.
[14] M. Priyan and G. U. Devi, A survey on internet of vehicles: applications, technologies, challenges and opportunities," *International Journal of Advanced Intelligence Paradigms*, vol. 12, no. 1-2, pp. 98–119, 2019.
[15] S. Kumar, H. Sharma, G. Singh, Neetu, and H. Chugh, Internet of vehicles (iov): A 5g connected car," *Advances and Applications in Mathematical Sciences*, Dec. 2019.
[16] A. Kumar, K. Rajalakshmi, S. Jain, A. Nayyar, and M. Abouhawwash, A novel heuristic simulation-optimization method for critical infrastructure in smart transportation systems," *International Journal of Communication Systems*, p. e4397, 2020.
[17] K. J. Borah, J. Borah, and M. Kantipudi, Optimal control of cyber physical vehicle systems," *International Journal of Intelligent Systems Design and Computing*, vol. 1, no. 3-4, pp. 205–213, 2017.
[18] S. Chaba, R. Kumar, R. Pant, and M. Dave, Secure and efficient key delivery in vanet using cloud and fog computing," in *2017 International Conference on Computer, Communications and Electronics (Comptelix).* IEEE, 2017, pp. 27–31.
[19] W. Xu, H. Zhou, N. Cheng, F. Lyu, W. Shi, J. Chen, and X. Shen, Internet of vehicles in big data era," *IEEE/CAA Journal of Automatica Sinica*, vol. 5, no. 1, pp. 19–35, 2017.
[20] X. Wang, Z. Ning, and L. Wang, Offloading in internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4568–4578, 2018.
[21] J. Kang, R. Yu, X. Huang, M. Jonsson, H. Bogucka, S. Gjessing, and Y. Zhang, Location privacy attacks and defenses in cloud-enabled internet of vehicles," *IEEE Wireless Communications*, vol. 23, no. 5, pp. 52–59, 2016.
[22] J. Kang, R. Yu, X. Huang, and Y. Zhang, Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, 2017.
[23] E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, Internet of vehicles: From intelligent grid to autonomous cars and vehicular fogs," *International Journal of Distributed Sensor Networks*, vol. 12, no. 9, p. 1550147716665500, 2016.
[24] W. Zhang, Z. Zhang, and H.-C. Chao, Cooperative fog computing for dealing with big data in the internet of vehicles: Architecture and hierarchical resource management," *IEEE Communications Magazine*, vol. 55, no. 12, pp. 60–67, 2017.
[25] A. Paul, A. Daniel, A. Ahmad, and S. Rho, Cooperative cognitive intelligence for internet of vehicles," *IEEE Systems Journal*, vol. 11, no. 3, pp. 1249–1258, 2015.
[26] P. M. Kumar, G. Manogaran, R. Sundarasekar, N. Chilamkurti, R. Varatharajan *et al.*, Ant colony optimization algorithm with internet of vehicles for intelligent traffic control system," *Computer Networks*, vol. 144, pp. 154–162, 2018.
[27] Y. Agarwal, K. Jain, and O. Karabasoglu, Smart vehicle monitoring and assistance using cloud computing in vehicular ad hoc networks," *International Journal of Transportation Science and Technology*, vol. 7, no. 1, pp. 60–73, 2018.
[28] S. Debroy, P. Samanta, A. Bashir, and M. Chatterjee, Speed-iot: spectrum aware energy efficient routing for device-to-device iot communication," *Future Generation Computer Systems*, vol. 93, pp. 833–848, 2019.
[29] E. Mouhcine, K. Mansouri, and Y. Mohamed, Intelligent vehicle routing system using vanet strategy combined with a distributed ant colony optimization," in *International Conference on Advanced Information Technology, Services and Systems.* Springer, 2018, pp. 230–237.
[30] C. J. Joshua, R. Duraisamy, and V. Varadarajan, A reputation based weighted clustering protocol in vanet: a multi-objective firefly approach," *Mobile Networks and Applications*, vol. 24, no. 4, pp. 1199–1209, 2019.
[31] M. Gupta, N. Sabharwal, P. Singla, J. Singh, and J. J. Rodrigues, Psarv: Particle swarm angular routing in vehicular ad hoc networks," in *International Conference on Wireless Intelligent and Distributed Environment for Communication.* Springer, 2018, pp. 115–127.
[32] X. Hu, T. Wu, and Y. Wang, Social coalition-based v2v broadcasting optimization algorithm in vanets," in *International Conference on Swarm Intelligence.* Springer, 2019, pp. 318–325.
[33] J. Toutouh and E. Alba, A swarm algorithm for collaborative traffic in vehicular networks," *Vehicular Communications*, vol. 12, pp. 127–137, 2018.
[34] R. C. Poonia, A performance evaluation of routing protocols for vehicular ad hoc networks with swarm intelligence," *International Journal of System Assurance Engineering and Management*, vol. 9, no. 4, pp. 830–835, 2018.
[35] R. Yarinezhad and A. Sarabi, A new routing algorithm for vehicular ad-hoc networks based on glowworm swarm optimization algorithm," *Journal of AI and Data Mining*, vol. 7, no. 1, pp. 69–76, 2019.
[36] S. Glass, I. Mahgoub, and M. Rathod, Leveraging manet-based cooperative cache discovery techniques in vanets: A survey and analysis," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2640–2661, 2017.
[37] L. Tuyisenge, M. Ayaida, S. Tohme, and L.-E. Afilal, Network architectures in internet of vehicles (iov): Review, protocols analysis, challenges and issues," in *International Conference on Internet of Vehicles.* Springer, 2018, pp. 3–13.
[38] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero Ibáñez, A seven-layered model architecture for internet of vehicles," *Journal of Information and Telecommunication*, vol. 1, no. 1, pp. 4–22, 2017.
[39] O. Senouci, Z. Aliouat, and S. Harous, A review of routing protocols in internet of vehicles and their challenges," *Sensor Review*, 2019.
[40] J. Contreras-Castillo, S. Zeadally, and J. A. Guerrero-Ibañez, Internet of vehicles: architecture, protocols, and security," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3701–3709, 2017.
[41] S. Vashist and S. Jain, Location-aware network of drones for consumer applications: Supporting efficient management between multiple drones," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 68–73, 2019.

[42] S. Kumar, D. Kaur, and M. Talwar, Comparative performance analysis of aodv, dsdv and zrp under various network density and traffic in manets," *Journal of Computer Technology & Applications*, vol. 7, no. 2, pp. 9–16, 2019.

[43] M.-S. Pan and S.-W. Yang, A lightweight and distributed geographic multicast routing protocol for iot applications," *Computer Networks*, vol. 112, pp. 95–107, 2017.

[44] A. Gulati, G. S. Aujla, R. Chaudhary, N. Kumar, and M. S. Obaidat, Deep learning-based content centric data dissemination scheme for internet of vehicles," in *2018 IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[45] M. S. Sheikh, J. Liang, and W. Wang, A survey of security services, attacks, and applications for vehicular ad hoc networks (vanets)," *Sensors*, vol. 19, no. 16, p. 3589, 2019.

Edited by: Anand Nayyar
Received: Apr 21, 2020
Accepted: Jul 1, 2020