Review on IoV (Internet of Vehicles) : Threats, Applications and Routing Protocols

Falah Noor[1], Dr. Pooja Sahni[2], Dr. Harpal Singh[3] , Dr. Sukhdeep Kaur[4]

[1]M.Tech (Scholar), Department of Electronics and Communication, Chandigarh Engineering College, Landran, Punjab, India
[2,3,4]Professor, Department of Electronics and Communication, Chandigarh Engineering College, Landran, Punjab, India

---***---

Abstract - *Due to the growth of vehicular activities in the current scenario, the mortality rate increased because of the accidents. More and more vehicles are increasing, which are associated with the IoVs making the network activities more challenging. Therefore IoV is the conjunction of internet transmission with IoT. It is a developing area of the automated manufacturing and essential section of the Smart-cities. Generally, IoV is a global system linking smart entities and is capable to connect them. When the smart objects are interconnected over the internet which are wholly vehicles, then IOT(internet of things) turns intoIOV (internet of vehicles). Generally, IoV is designed to address and resolve various issues by encouraging the goal of fewer accidents, less energy dissipation, less emission, high efficiency by the development of the automobiles and communication (transportation) scheme.However, some of the applications of IoV are; traffic guideline scheme, secure navigation, intelligent vehicle control, reducing congestion and accidents, electronic toll collection, monitoring of the traffic flow.In this research, an overview of the internet of vehicles (IoV) is described. Besides, the architecture of IoV consisting of various layers,the security and privacy issues is also clarified in this research. Moreover, various threats and applications in IOV are also enlightened along with routing protocols, including unicast, geo-cast and multicast and their sub types.*

Key Words: Internte of Vehicles, Internet of Things, Routing Protocols, Security Threats and Applications.

1.INTRODUCTION

An urban population is increasing and fast development of the metropolises,vehicles is increasing at a faster rate. There has been a huge growth in the arrangement of the EV (electric vehicles), both are wholly electric and plug-in hybrids.There is a requirement of the improved communications and inter connectivity between these vehicles because of the high mobility rate [1]. The vehicles change from a normal mean of transport to smart objects with detection and communication aptitudes, that has become an essential part of the advanced city [2]. The advanced vehicles demonstrate five characteristics; self-driving, social-driving, electrical-vehicles, and portable requests.IoTis a globalized system linking advanced entities and allowing them to connect [3]. When the advanced entities are linked over the internet as vehicles, then IoT becomes IoV (internet of vehicles). IoV is an advanced application of IoT in intellectual transport scheme [4]. It is intended to reserve as significant information sensing and handling platform for intelligent transport schemes.IoV contains vehicles that are connected as well as have the sensor devices that are supported by pedestrians, RSU(roadside units), and the unrestricted networks through V2V, V2R (vehicle-to-road), V2H (vehicle-to-human) and V2S (vehicle-to-sensor) interconnectivity. IoV is determined as the sub-group of the VANET that is established from MANET.It has been researched that network architecture ofIoV is based on IoT, which is similar to IoV and contains various layers such as sensing layer(SL), network layer(NL), and application layer(AL). Conversely, IoV is a complex network that contains the features of a social vehicle environment that firmly coordinate interaction and dynamic evolution [5]. The given figure 1, described the vehicle network setting detecting and controller layer, NAL (Network Access Layer), coordinate calculating and application layer (AL).

1.1 Vehicular System Environment Detecting

It is the detection based on the IOV applications, like application of the automated vehicle, IT: Intelligent Traffic, and vehicular data. The controller of the vehicle and environment traffic is based on IoVimplementation [6]. The traffic-environment is sensed from the view point of the vehicles through autopilot, traffic jam scheme. This layer determines the method to screen and eliminate different active data of social beings, vehicles, and the environment by sensing technology. Moreover, it focused on the method to get and perform coordinate regulation guidelines and after that feedback outcome to co-operative regulation. In the final process, it develops the abilities of the swarm sensing method and partakes sensing in a unique model.

1.2 System Access and Transport Layer

The major purpose of the transport layer is to determine the network access, information processing and examine packet transmission. Simultaneously, it may recognize the remote monitoring and maintenance of the nodes in IOV. The other goal of this layer is to determine the interlinking and data interchange, that contains the access network, the broadcast, and the control scheme [7]. The access system delivers an actual time, 3- dimension, heterogeneous system access for vehicular concerning the scheme. The broadcasting and controlled scheme reply to report access sources and balanced data load. After that, it develops a static, superior data and communication channel measuring the system load situations and access source restraints.

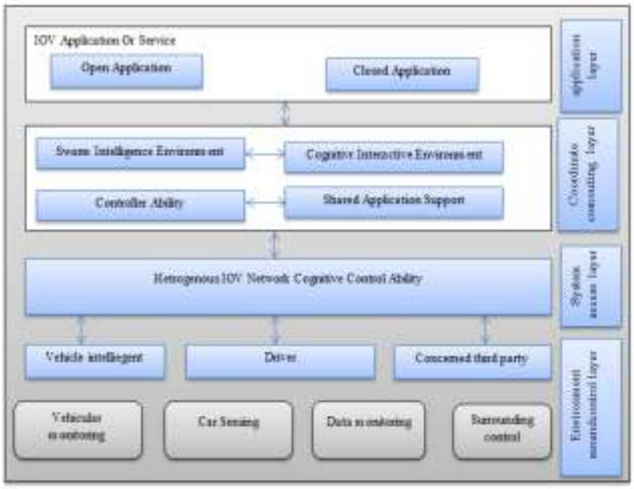
IOV Application Or Service
Open Application
Closed Application
application layer
Swarm Intelligence Environment
Cognitive Interactive Environment
Controller Ability
Shared Application Support
Coordinate computing layer
Heterogenous IOV Network Cognitive Control Ability
System access layer
Vehicle intelligent
Driver
Concerned third party
Vehicular monitoring
Car Sensing
Data monitoring
Surrounding control
Environment monitor/control layer

Figure - 1. Architecture of IoV.

1.3 Coordinated Computed Control Layer

In this layer, the applications include the system-wide ability to coordinate computation and control of the social vehicular environment, like as information processing, source-allocation, and swarm intelligence computation. After the viewpoint of IOV object coordinates a particular model, the control layer presents the ability of social vehicle coordinates computation control to preserve human vehicles, which gets coordination into IOV environment. Based on the coordinate swarm model, this layer must provide the ability, consisting of multi-human and multi-vehicles coordinate control application environments [8]. Moreover, to achieve co-ordinates control needs, the layer must provide the ability of communication co-ordinated maintenance.

1.3 Application layer

This layer of IoV offers different kinds of applications to acquire the needs of human vehicle co-ordinates. Moreover, the application layer may be free and must share data to provide new applications and corporate operating methods. Generally, the application layer may be categorized into open and close applications [9] [10]. The close application is interrelated to special industrial services, like intelligent-traffic requests and controlled platforms. The open application contains different existing services like real-time traffic applications presented by different internet service providers. This layer presents an open application to third party suppliers. In Table 1, various layers are described with their components and technologies. The different layers are given as the AL, communication layer, security layer, integration layer, and embedded layer. The application layer includes the data and vehicular monitoring, and environmental control.

Table 1 - Several layers with Elements and Technologies

Layer	Elements	Explanation	Technologies
Application layer	Vehicular storing sensor, traffic control device, smart home device.	Sensor devices are utilized to identify different data and transmit signals to the receiver.	Cloud and computing application, smart sensors
Access control layer	Access control, device identification, transmission and storing	Enable transmission among smart sensors and IOV.	Co-ordinate access point sensors
Entrenched layer	H/W and mechanical devices	Monitor and process different sensor devices	Actuators and sensors
Transferring layer	Communication and system devices	Gather data that transferred to the receiver node.	Wireless WAN, satellite system.
Security layer	Secure device and embedded	Provide IOVto a malicious user.	Cryptographic technology.
Integral layer	Interact and API for the fog to cloud -server	Provide computing to the cloud server.	Web services

2. LITERATURE SURVEY

Dandala, T. T et al., 2017[11] proposed a research system model in IoVs, discussed the tools need to generate the internet of vehicles, presented various applications that depend on existing technologies, various open research issues and described various further research areas of IoV. This research recognized the potential benefits pretended by the concept of IoV over the tradition of things in IoV (internet of things) in traffic maintenance. This research was projected to advise a more effective method of traffic maintenance and making road movement in a better way. This research was used in better structure and methods for road traffic management and make an influence on the efficiency of monitoring and emergency reply to traffic incidents. **Gasmi, R et al., 2019[12]**clarified main variations among VANET and IoV in various factors. Firstly, they defined the variation among VANET communication structure and IoV communication structure. After that, they referred to the system technologies that present in VANET and IoV environment. In the next procedure, they explained the cloud-based communication in IoV systems. In the final approach, they illustrated the protocol stack of every scheme. In this research, they provided the main variation among VANET and IOV. Initially, they recognized the variance among the VANET and IoV communication structure. They found that IOV contains a large amount of the kind of communication comparable to VANET.**Wang, J et al., 2018 [13]**developed a weigh and un-directed graph method for IoV sensing system and verified the time-invariant complexity features that depend on the actual time GPS database.They examined the traffic data assortment and dispersion issues of IoV systems. Above all else, they inspected the qualities of the GPS dataset of Beijing city taxis and checked both the time-invariant little world behaviour and the sans-scale property of the IoV arrange. Besides, they characterized Connection Record Traffic Data Stream of Each Connection. Traffic data stream concerning each connection parameterized by various connection ability. The connection/hub correspondence impedance and evaluated the data assortment and dispersal execution. At long last, they proposed an IoV supported nearby traffic assortment design, a portal determination plot for data assortment just as an ideal traffic information transmission model for urban traffic control and maintenance. The experiment outcome showed that fewer vehicles worked as gateways and only a few routes are chosen as data communication routes in different IoV vehicle schemes to acquire enhanced performance and less communication cost.**Lu, H. et al., 2019 [14]**presented research on cloud calculation patterns and IoT artificial intelligence schemes. They proposed a cross-domain output for automated driving. On another hand to current research, that mainly focused on communication technologies, the output received intellectual and consistent automated driving job processing and improves communication performance using cognitive IoV. Moreover, they overviewed the enabling technologies and structure of cognitive IoV for automated driving. In addition, they described the automated driving cognitive IoV mainly from the view and process of computation. Simulation results are then evaluated to determine the influence of the cognitive IoV for automated driving. Generally, the research explored the rates and prospects of cognitive IoV in automated driving. **Singh, D et al.,2015[15]**specified the interconnected vehicular structure outputs for both secure and smart driving in private or public vehicles.The thought was to use the Web of vehicle's dash-board digital camera to enhance the controller and accident prevention or checking managements. The brilliant Eye has the ability to catch and share their constant accident or traffic film into content, sound and video structures to the related specialists, for example, closest vehicles, police staff, medical clinics, relatives and insurance agencies in a split second alongside the area. Subsequently, the Shrewd Eye arrangements can provide car markets for brilliant and safe driving.**Yan, C et al.,2016 [16]**proposed research on the enhanced traditional ZRP algorithmic in maintaining route and finding algorithm, decreasing the transmission frequency and enhancing the information communication route, that would present experience in applying the transmission scientific method for intelligent transmission. Meantime, this approach has some benefits. The time when the amount of nodes becomes large, the secret and the topology management approach would be essential to reconstruct since only single CH was not sufficient to see the computation requirement. In table 2, the comparative analysis of different techniques, advantages, and issues, along with metrics are explained.

Table 2: Evaluation based on techniques, benefits, issues and Parameter Metrics

Author'sName	**Technique**	**Benefits**	**Issues**	**Metrics**
Dandala, T. T Et Al., 2017[11]	Traffic Management	Traffic Control, Emergency Reply	Failure Of Network	-
Gasmi, R Et Al., 2019[12]	Cloud-Based IOV Model	Diver Assistance And Security	Congested Network	-
Wang, J Et Al., 2018 [13]	Weigh And Undirected Graph Method	Traffic Data Collection	Network Failure	Latitude Selection Probability
Lu, H. Et Al., 2019 [14]	Automated Driving Model	Cloud Processing	Design And Cross-Domain Issue	Accuracy And Delay
Singh, D Et Al., 2015 [15]	Interconnected Vehicular Structure	Improve Security Of Vehicle	Number Of Accidents	-
Yan, C Et Al., 2016 [16]	Zone Routing Method	Network Control And Data Efficiency	High Energy Depletion	PDR, Delay, And Route Consumption

3. INTERNET OF VEHICLES SECURITY ISSUES

A most important part of the network and associated vehicles is safety. Due to lot of attacks nowadays, it's hard to operate networks and associated devices. More security problems may cause unnecessary accidents and harmful injuries. In vehicular ad hoc networks, vehicles may disseminate valuable data regarding different essential actions, like road situations, congestion rates, accidents and dispersed traffic maintenance [17]. Vehicles may receive the data packets with the communication to the other vehicles or networks to identify the traffic jamming and collisions. During serious situations, the availability of malicious hops may lead to fake data dissemination in the network, which may compromise the security and privacy of the prospective operators.

3.1 Security Fundamentals:

The number of issues in security can be occurred as in the IoV, the data need to be transmitted with a small amount of time to the other part of the network. The data forwarded must be authenticated and encrypted; it may not leak private data about the operators; therefore, violating the right to privacy of the user. There are different security fundamentals in IOVare [18]:

User legitimacy: The sources of data may be genuine as well as a malicious hop. In case the hop is malicious or genuine, the first stage is enhancing the security of IOV network. The network must be capable to differentiate the attacked and normal calls from the network to take security actions accordingly.

User Privacy: Generally, the data message may not consist of any data about the source.It should be more secure while broadcast over a network and the information about transmitting end will be secured.

User Reliability: The information reached to the destination must exactly as information forwarded through the source node [19]. The network must be capable to assure that some attackers have not interfered with the data message forwarded by the source node. The network must be capable to assure that some attacker has not interfered with data when passed through the network medium.

Lower Overhead: The data messages are not valuable if it is not stored in the destination in the specified time. Consequently, the IOV scheme must assure that the overhead may not be increased,even though it focused on security. It is due to the fact that consumes more time at the time of broadcasting data and unless it reaches the receiver node, it becomes invaluable.

4. DIFFERENT THREATS AND APPLICATIONS IN IoV

Generally, the IoV network may get threatened from different of aspects by various methods such as congestion, interfering, eaves-dropping and so forth, which deceasing the consistency, strength, security, and privacy of IoV. Hence, the network may lose the capability to present efficient service, and may also lead to severe accidents because of the non-uniform dissemination of the hops, perception of information. Various types of attacks are described as;

4.1 Threats on Authentication:

Sybil Threat:

In the sensor network, a single hop with numerous identifications may destroy the network by regulating large areas in the network. Generally, the vehicles may access IOV for the moment and unstably and this is the main reason that capable the Sybil hops to find the chance to attack [20]. The standard vehicles are simpler to be threatened and vehicles may not have their own standard services and personal information of the vehicles is escaped.

GPS Fraud:

In this, the GPS may be provided with fraud data about the position, velocity and other GPS data. Whenever this data has been received by the services about security and economic problems, the opponent may pretend enough false, ut unable to deny proofs to escape from tracing. In IOV, the GPS data has a vital location in various applications like navigation tools and payment benefits and the incorrect position may lead to fraud-proof and changeable features destruction.

Masquerading Threat:

In a standard system environment, a single entity contains exceptional identification. This threat may affect a large number of hops in such a condition to have the same ID. Consequently, the IOV scheme may not work properly and have an unordered network [21].

Wormhole Threat:

This type of threat always has a serious effect on the IoV network because of the features of variations and huge requirements of the effective routing algorithm. Each kind of IoVcomponents may lose the standard response if it is attacked by wormholes.

4.2 Accessibility Threats:

The threats such as the denial of service(DOS)and channel intrusion(CI) are the major types of threats on obtain ability. This kind of threat essentially uses the limits of bandwidth and transmission energy to make IOV scheme collapse [22]. A large number of the essential elements of IOVare uncovered outside and may have incomplete security, as a result, it is facile to be delayed, control and wholly damaged. The effect of the accessibility threat is based on the kind of the hops to be threatened i.e destruction of the core unit may have a high impact on IOV scheme than the damaged vehicle.

4.3 Secrecy Threats:

The information and data sources are always an essential part of the scheme and secrecy is required to assure that the delicate information may only be accessed by the fair hops which are approved in the correct way. The secrecy threat stole the information through eavesdropping or interception [23]. An intruder compromises the standard entity in most of the cases such as vehicle or RSU. After that, the intruder may have the capability to access the secret sources by eves-dropping this entity, which may result in the leakage of the privacy of the user.

4.4 Routing Threats:

Various kinds of threat in the routing method is available that includes eavesdropping, denial of service(DOS), Masquerading, route variations. The routing algorithm and its quality suggest the influence of the IoV communication between RSU, vehicles and routing methods of IoV is complex because of the limitations which are bandwidth, transmission energy, and mobility rate. Hence, the complexity may result in the vulnerability of the IoV routing methods.

4.5 Information authenticity Threats:

Whenever data packets are transferred in the system, it is essential to assure that source information has not been altered.Information authenticity threats may be considered into different types which are, replay threat, tampering with data message and illusion threat. The features of directness make IoV information simple to be broadcasted, mainly in routing and wireless communication. Information authenticity Threats marks the applications of IOV not reliable and this damage may have an insightful and enduring influence on IOV.

4.6 APPLICATIONS IN IoV

IoV is used in a variety of applications such as discussed as follows:

Secure driving: This relates to a co-operative collision prevention scheme that used sensors to identify approaching collision and provides an alert message to the driver. This service includes periodical status and emergency data messages. An emergency data message is activated by emergency events like traffic jams, accident and so forth.

Traffic controller: IOV presents the necessary changes to urban congestion,maintenance, transport, and urban traffic. **Crash Reply:**The interconnected vehicles may automatically forwards the real-time information about the crash with vehicle position to emergency groups. An accelerating emergency reply may save many lives.

Suitability application: The capability to remotely access a vehicle makes probable application like as unlock the remote door and stolen vehicle retrieval [24]. The interconnected vehicle technology may present transportation agencies with enhanced real-time traffic, make it simpler to maintain transportation schemes for deducted traffic and congestion. **Infotainment:** The interconnected vehicles may provide online, in-vehicle, entertaining choices that provide flowing music and data through the control panel.

Other uses include electric toll collection, traffic direction scheme, secure navigation, intelligent vehicle regulation, crash avoidance, and traffic flow monitoring.

5. SEVERAL ROUTING PROTOCOLS AND ITS TYPES

In this section some of the routing protocols of IOV are described such as Uni-cast, broadcast, etc routing protocols.

5.1 Unicast Routing Protocols:

The main objective of this protocol is to transfer information from one source to one destination through the multi hop, either by a node to node greedy forwarding method or carry and forward method. The middle vehicles on the route must delay data as soon as possible for the sender to the receiver. Later, it may contain information unless a forwarding decision is made by the routing approach. Generally, the unicast routing may be topology, location, route based routing. This protocol includes;

5.1.1 VADD (Vehicle assists data delivery routing protocol)

This protocol used carry and forward methods to route information from the sender and receiver, this protocol deals with the issue of higher mobility and frequent interruption. This protocol was suitable only at the time when the sender is movable and the receiver is stable. The main work of the VAAD is to identify the forwarding route with a small packet delivery delay [25]. In given fig, vehicle v1is nearest to intersection I1that required to forward the data packet to shop nearer to intersection I2. The two probable routes to transfer data packet to a destination, hop I1 and I2 and I1, I3 andI4. After the computation of the delay method using data is measured by digital maps. VADD may select I1, I3, and I4 which is denser than the old route, though I1 and I2 are least than I1, I3, I4.

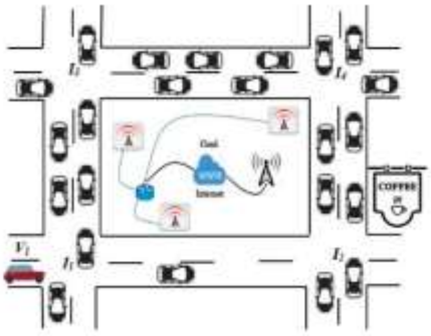

Fig.2 Design of VADD protocol [26]

5.1.2 CAR(Connectivity aware routing)Protocol

This protocol is a position-based routing method that builds a route between the sender and receiver by engaging the middle connections.

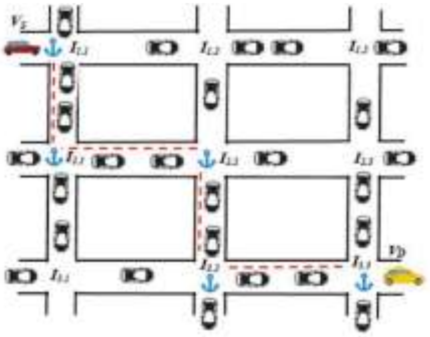

Fig.3 Design of CAR protocol [26]

This protocol is beneficial to the city and highway environments. For instance, the CAR protocol computing process is given in the figure. For instance, in the CAR protocol data packet is forwarded from the sender to the receiver. The complete care by the searching data packet, record the identity. When finding the data packet reaches the destination, it selects the best route with maximum density and forwards a response to the sender. All the connections through the data packets are forwarded, may be labelled as anchor points. In the end, data packets have forwarded the route through already selected lists of anchor-points.

5.1.3 Geo-cast Routing Protocols

It is mainly position based multicast routing. The main goal of this method is to forward a data packet from sender all neighbor nodes with an identified geographical area, that is called the zone. This protocol is implemented through the multicast application by considering multicast collection to the group of hops in the required geographical area [26]. Generally, this protocol forwards an alert message to other vehicles that are positioned in the region of risk on the highway by choosing a relay hop that is based defer-time approach.

5.1.4 TL-TSGR(Traffic light-based time stable geo-cast routing)protocol

Generally, the traffic lights are beneficial in geo-cast routing. This protocol is used for notifying vehicles after an accident in urban vehicle environment. Through the use of traffic light behavior and vehicular distribution data, the chance of the accident is analyzed. It has been observed that it has a low end to end delay compared to the normal flooding method.

5.1.5 DRG(Distributed robust geo-cast routing) protocol

This protocol is used for inter-vehicle communication. Its main objective is to forward a data packet to vehicles positioned in a specified static geographical area. Vehicles may get or lose data packets under the existing position of the node. DRG mainly adapts itself to system topology and assures high delivery rate in the sparse system during high overhead, when it forwards data packet effectively in a dense network.

5.1.6 Broadcast Routing Protocols

This protocol is used to share traffic, weather and road situation data between vehicles, and to forward announcements and proclamations. It is also utilized route discovery stage to search an efficient path to destination hop. When a data message is required to be disseminated to vehicles away from the direct communication range, the multi-node system is utilized.

5.1.7 UMB (Urban Multi –node Broadcast Routing) protocol

This protocol is measured to address the problem-related broadcast storms, hidden hops, and consisting of multi-node broadcasts in urban regions. It consists of two stages, indication and intersection broadcast [27]. In the initial stage, the source selects the last hop without considering the ID or location of neighbors. In other stages, the repeaters stored the connection that sends the data packet to other road segments. The given figure demonstrates that vehicle A used, the indication broadcast to reach vehicle B. Hence, A is out of the communication range of repeater C but B is placed in the range when connected to C. When C gets the message, it starts connection broadcast to N (north) and S (south) directions. Meanwhile, repeater D is also given in the communication range of C, C also forwards the data packet to D.

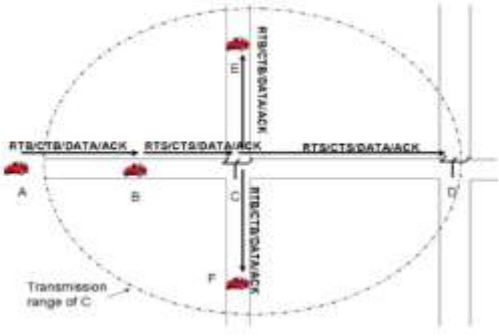

Fig. 4 Design of UMB protocol [26][27]

5.1.8 DVB (Distributed Vehicular broadcast protocol)

This protocol is a multi-node broadcast routing protocol. It is appropriate for the dense and sparse traffic situations on the highway and may decrease the broadcasting overhead accordingly. This protocol broadcasts both deep and unconnected systems issues in urban regions in a VANET indirect delay multi-node transmissions an indirect delay by store carry forward method. This protocol is mainly used in urban areas in VANET.In table 3, various routing protocols in IoV are given with a detailed description. Moreover, the type of the protocol, information, condition, scenario, and the network are elaborated.

Table 3: Routing protocols in IoV [28] [29]

Method	Type and Data	Situation	Scenario	Network
DSDV	unicast Topology based	Delay sensitive	One or two dimension	homogeno us
DSR	unicast Topology based	Delay sensitive	One or two dimension	homogeno us
AODV	unicast Topology based	Delay sensitive	One or two dimension	homogeno us
GPSR	unicast Topology based	Delay sensitive	two dimension	homogeno us
IVG	Geo-cast Position based	Delay sensitive	one dimension	homogeno us
Geo SPIN	Geo-cast Position based	Delay Tolerant	one dimension	homogeno us
DV-CAST	Broadcast Map based	Delay - Tolerant	one dimension	homogeno us
BROAD COMM	Broadcast NA	Delay - sensitive	one dimension	homogeno us
Double-Timer based	Broadcast Position based	Delay - sensitive	one dimension	homogeno us
IGRP	Unicast Position based	Delay - sensitive	one dimension	homogeno us
IEGRP	Unicast Position based	Delay - Tolerant	Two dimension	homogeno us
SDMA	Unicast Position based	Delay - Tolerant	Two dimension	homogeno us

6. CONCLUSION

In conclusion, with the huge growth of internet and communication technologies, vehicles may often move at a faster rate in cities and have strong working out and communication capabilities. IoV is developing as an essential component of the smart cities being technologically advanced all over the world. IoV is a composite integrated network scheme that connects individuals in and nearby vehicles, smart schemes on board automobiles and different cyber mechanical schemes in urban environments. With the increasing number of vehicles, the era of IoT is transformed into IoV (internet of vehicles). IoV has attracted the interest of a large number of industries and investigators because of the huge growth of computation, communication and transport technologies. This research discussed current technologies, applications and security aspects in the region of IoV. This research described various layers of IoV that are considered in a layered architecture measuring the functionalities and demonstrations of every layer. In addition, various threats ofIoV along with existing applications are also explained. Besides, this research aimed to present a review on different routing protocols that are classified as a unicast, geo-cast and broadcast routing protocol. Moreover, the subtypes of unicast, geo-cast and broadcast routing protocol are also described. IoV comprises not only traditional VANET, that regularly include small-scale and heterogeneous system, but also large-scale networks such as Metropolitan and Adhoc. Generally, the arrangement of the traditional routing protocols would be a promising aspect in the future.

REFERENCES

[1] Maglaras, L. A., Al-Bayatti, A. H., He, Y., Wagner, I. and Janicke, H. (2016), " Social internet of vehicles for smart cities," Journal of Sensor and Actuator Networks, 5(1), 3.

[2] Kang, J., Yu, R., Huang, X. and Zhang, Y. (2017), " Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," IEEE Transactions on Intelligent Transportation Systems, 19(8), 2627-2637.

[3] Sadiku, M. N., Tembely, M., & Musa, S. M. (2018), " Internet of vehicles: An introduction," International Journal of Advanced Research in Computer Science and Software Engineering, 8(1), 11.

[4] Yang, F., Wang, S., Li, J., Liu, Z. and Sun, Q. (2014), " An overview of internet of vehicles," China communications, 11(10), 1-15.

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

[6] Contreras-Castillo, J., Zeadally, S. and Guerrero-Iba�z, J. A. (2017), " Internet of vehicles: architecture, protocols, and security," IEEE Internet of Things Journal, 5(5), 3701-3709.

[7] Tuyisenge, L., Ayaida, M., Tohme, S and Afilal, L. E. (2018), " Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues," In International Conference on Internet of Vehicles (pp. 3-13). Springer, Cham.

[8] Butt, T. A., Iqbal, R., Shah, S. C and Umar, T. (2018), " Social Internet of Vehicles: Architecture and enabling technologies," Computers & Electrical Engineering, 69, 68-84.

[9] Ang, L. M., Seng, K. P., Ijemaru, G. K and Zungeru, A. M. (2018), "Deployment of IoV for smart cities: applications, architecture, and challenges,"IEEE Access, 7, 6473-6492.

[10] Butt, T. A., Iqbal, R., Shah, S. C and Umar, T. (2018), "Social Internet of Vehicles: Architecture and enabling technologies," Computers & Electrical Engineering, 69, 68-84.virtualization with SR-IOV. Journal of Parallel and Distributed Computing, 72(11), 1471-1480.

[11] Dandala, T. T., Krishnamurthy, V and Alwan, R. (2017), " Internet of Vehicles (IoV) for traffic management," In 2017 International Conference on Computer, Communication and Signal Processing (ICCCSP) (pp. 1-4). IEEE.

[12] Gasmi, R and Aliouat, M. (2019), " Vehicular Ad Hoc NETworks versus Internet of Vehicles-A Comparative View," In 2019 International Conference on Networking and Advanced Systems (ICNAS) (pp. 1-6). IEEE.

[13] Wang, J., Jiang, C., Han, Z., Ren, Y and Hanzo, L. (2018), "Internet of vehicles: Sensing-aided transportation

information collection and diffusion," IEEE Transactions on Vehicular Technology, 67(5), 3813-3825.

[14] Lu, H., Liu, Q., Tian, D., Li, Y., Kim, H and Serikawa, S. (2019), " The cognitive internet of vehicles for autonomous driving," IEEE Network, 33(3), 65-73.

[15] Singh, D. and Singh, M. (2015), " Internet of vehicles for smart and safe driving," In 2015 international conference on connected vehicles and expo (ICCVE) (pp. 328-329). IEEE.

[16] Yan, C., Wang, J. and Li, Z. (2016), " Research on traffic information transmission algorithm in internet of vehicles," In 2016 IEEE International Conference on Intelligent Transportation Engineering (ICITE) (pp. 147-150). IEEE.

[17] Chen, Y. R., Sha, J. R and Zhou, Z. H. (2019), "IOV Privacy Protection System Based on Double-Layered Chains," Wireless Communications and Mobile Computing, 2019.

[18] Sharma, N., Chauhan, N and Chand, N. (2018), " Security challenges in Internet of Vehicles (IoV) environment," In 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC) (pp. 203-207). IEEE.

[19] Abu Talib, M., Abbas, S., Nasir, Q. and Mowakeh, M. F. (2018), " Systematic literature review on Internet-of-Vehicles communication security," International Journal of Distributed Sensor Networks, 14(12), 1550147718815054.

[20] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L and Xiong, Y. (2015), " Security and Privacy in the Internet of Vehicles," In 2015 International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI) (pp. 116-121). IEEE.

[21] Sun, Y., Wu, L., Wu, S., Li, S., Zhang, T., Zhang, L and Cui, X. (2017), " Attacks and countermeasures in the internet of vehicles," Annals of Telecommunications, 72(5-6), 283-295.

[22] Makhdoom, I., Abolhasan, M., Lipman, J., Liu, R. P and Ni, W. (2018), " Anatomy of threats to the internet of things," IEEE Communications Surveys & Tutorials, 21(2), 1636-1675.

[23] Buinevich, M and Vladyko, A. (2019), "Forecasting Issues of Wireless Communication Networks' Cyber Resilience for An Intelligent Transportation System: An Overview of Cyber Attacks," Information, 10(1), 27.

[24] Wu, W., Yang, Z and Li, K. (2016), " Internet of Vehicles and applications," In Internet of Things (pp. 299-317). Morgan Kaufmann.

[25] Alouache, L., Nguyen, N., Aliouat, M and Chelouah, R. (2019), " Survey on IoV routing protocols: Security and network architecture," International Journal of Communication Systems, 32(2), e3849.

[26] Cheng, J., Cheng, J., Zhou, M., Liu, F., Gao, S and Liu, C. (2015), " Routing in internet of vehicles: A review," IEEE Transactions on Intelligent Transportation Systems, 16(5), 2339-2352.

[27] Wang, C., Zhang, L., Li, Z and Jiang, C. (2018), "SDCoR: Software defined cognitive routing for Internet of vehicles," IEEE Internet of Things Journal, 5(5), 3513-3520.

[28] Priyan, M. K. and Devi, G. U. (2019), " A survey on internet of vehicles: applications, technologies, challenges and opportunities," International Journal of Advanced Intelligence Paradigms, 12(1-2), 98-119.

[29] Vuyyuru, R. and Oguchi, K. (2007), "Vehicle-to-vehicle ad hoc communication protocol evaluation using realistic simulation framework," In 2007 Fourth Annual Conference on Wireless on Demand Network Systems and Services (pp. 100-106). IEEE.