ISSN 1846-6168 (Print), ISSN 1848-5588 (Online)
https://doi.org/10.31803/tg-20210205104516

Subject review

Evolution of VANETS to IoV: Applications and Challenges

Faisal Rasheed Lone*, Harsh Kumar Verma, Krishna Pal Sharma

Abstract: Advancement in wireless communication technology along with the evolution of low power computational devices, have given rise to the Internet of things paradigm. This paradigm is transforming conventional VANETs into Internet-of- vehicles. This transition has led to a substantial commercial interest; as a result, there has been a significant boost in the field of the Internet of vehicles during the past few years. IoV promises a wide range of applications of commercial interest as well as public entertainment and convenience (collision warning systems, on-demand in-car entertainment, smart parking, traffic information). Applications related to vehicular and passenger safety are particularly of great commercial as well as a research interest as such IoV is going to be a core component in implementing the smart city concept. This paper gives an overview of the transition of conventional VANETs to IoV and highlights the potential applications and challenges faced by the Internet of Vehicles (IoV) paradigm.

Keywords: IoT; IoV; Security; VANET

1 INTRODUCTION

Of the 25-30 billion things envisioned to be connected to the Internet by 2020 [1], vehicles will contribute a compelling number. IoV is considered as a unique application of the Internet of Things (IoT). IoV is a dynamic mobile network establishing communication between heterogeneous networks using Vehicle-to-Vehicle (V2V), Vehicle-to-Roadside (V2R), Vehicle-to-humans (V2H), Vehicle-to-Sensors (V2S) and Vehicle-to-Infrastructure (V2I) [2, 3]. V2X (Vehicle to everything) communication will form the backbone of the Intelligent transportation systems [4, 5]. Conventional VANETs are transforming into the Internet of vehicles. While as VANETs consist of only vehicles connected in an ad-hoc manner exchanging data with each other, IoV spans a bigger network involving entities such as humans, things and other heterogeneous networks. IoV improves upon VANETs by incorporating cellular networks such as LTE, 5G etc., to provide an expansive and reliable communication. IoV uses ad-hoc networks for communication with infrastructure and a cellular network for communication with the backbone network [6, 7]. IoV enables data collection and sharing about surroundings, vehicles, road conditions [8].

Over the years, not much interest has been shown in VANETs as it was not able to provide global sustainable applications and services to users. Nevertheless, with the emergence of IoV, the desired commercial interests have begun to emerge. VANETs can thus be considered as a subset of IoV [9], offering more expansive coverage and application as such IoV is capable of providing services to a much larger area, such as a city or even a country. In comparison to VANETs, IoV treats a vehicle as a smart-entity equipped with various sensors and computational capability. The purpose of the IoV is to assimilate humans, vehicles, things and other heterogeneous networks to boost efficiency, security and safety of transport systems, to provide various services to a smart city (e.g. parking information, traffic information), services to users (e.g. on-demand in-car entertainment, remote diagnostics) and several other useful applications [10, 11].

IoV has brought about an opportunity to improve passenger safety and mobility by utilizing vehicular communication.

The importance of IoV can be highlighted by the Vehicle Infrastructure Integration program (VII), developed by the US department of transportation (DOT), acting as a prime component of the Intelligent Transportation System. The main objective of the program was to develop a wireless communication system to support the Vehicle to Vehicle and Vehicle to Infrastructure communications to enhance safety and traffic mobility [12].

Taking into account the immense benefits offered by IoV and the enormous number of vehicular nodes, it is evident that IoV is going to be one of the largest and most complex networks in the near future. With the decline in prices of electronic components and a neat amalgamation of these onboard devices present immense business opportunities, but at the same time give rise to intimidating research challenges. These issues might look akin to the ones faced in traditional ad-hoc networks, but various inherent characteristics such as the immense size of the network, speed of the vehicular nodes, intermittent connectivity,safety-critical applications, give rise to novel challenges as well as amplify the severity of traditional issues.

The paper is organized in the following way. In Section 2, we present the related work in the field. Section 3 describes the general architecture of IoV, followed by Applications of IoV in Section 4. In Section 5, we give an overview of various challenges faced by the IoV paradigm, and section 6 finally concludes the paper.

2 LITERATURE SURVEY

A common question usually faced is "How is IoV different from IoT and Wireless networks?". The answer lies in the fact that some characteristics of IoV are quite different when compared to IoT and wireless networks. A VANET transforms a vehicle into a mobile router [13]. Both wireless networks and IoV consist of mobile nodes. However, the trajectory followed by the nodes in IoV consists of a defined path which is subject to the road network of an area. In

contrast, the trajectory followed by nodes in a mobile network has no defined path and follow a random walk model. Moreover, IoT lays more stress on *"things"* and *"data awareness"* of these things, while as the main motive of IoV is to integrate humans and vehicles, where vehicles may be considered as an extension of human's capabilities. IoV connects vehicles, humans in and around the Vehicle, systems onboard the Vehicle by incorporating the sensors, vehicles and mobile devices forming a global network enabling it to deliver services and applications to humans around or onboard the Vehicle.

With the growth and advancement of wireless technologies, we can think of integrating vehicles in the network, thus constituting the Internet of Vehicles environment. Communication is made possible by incorporating short as well as long-range communication technologies [14] Many existing wireless technologies can be used to implement the IoV paradigm, including WLAN's, WIMAX, cellular wireless as well as satellite communications. Much research is focused on the wireless aspect of IoV, as a robust wireless scheme can immensely enhance the implementation of IoV by providing relatively better Quality of service (QoS). Each of the current crops of wireless technologies has their share of merits and demerits as far as IoV is concerned.

WLAN has achieved a lot of significance and approval in the market due to robust short-range communication, including high-speed transmissions. WLAN consists of IEEE 802.11 a/b/g/n/ac standards [8] each with a different capacity, modulation technology, bandwidth and coverage area. Performance analysis of IEEE 802.11 a, b, g in-car communication scheme showed that velocity up to 180 km/h has almost negligible impact on the performance [15]. Due to its shorter range, WLAN cannot sustain a VANET for longer duration due to constant movement of vehicles, leading to frequent topology changes. Performance of 802.11p based protocol in Vehicle to vehicle safety applications was analyzed in [16].

Table 1 Comparison of IEEE 802.11 Standards

IEEE 802.11 Standard	Operating Frequency (GHz)	Bandwidth	Beamforming	Coverage	Capacity	Interference	Quality
a	2.4	20	No	Low	Low	High on 2.4/Low on 5	Low
	5						
b	2.4	22	No	Low	Low	High	Low
g	2.4	20	No	Low	Low	High	Low
n	2.4/5	20	Yes	Low	Low	High on 2.4/Low on 5	Low
		40					
ac	5	20	Yes	High	High	Low	High
		40					
		60					
		80					

WiMAX covers IEEE 802.16 a/e/m standards which can cover more than 50 km/h of geographical area and can deliver a theoretical bandwidth up to 72 Mbps [15]. The IEEE 802.16 standard provides support for fixed broadband wireless only. In contrast, as IEEE 802.16e/mobile version supports mobility up to speeds of 160 km/h and various QoS provisions for non-line of sight communications [15]. The leverage WIMAX offers over WLAN is that a user need not frequently compete for entry into the network, instead only once during initial entry. Cellular wireless possesses a considerable potential for IoV due to its widespread penetration and already established robust infrastructure. The cellular network comprises of older technologies such as 3G, 4G, LTE, and more recently 5G. The third-generation networks (3G) are capable of delivering peak data rates of up to 3 Mbps in fixed and 384 Kbps in the mobile environment [17]. Tab. 1 compares the parameters of various IEEE 802.11 standards.

Authors in [18] evaluated the performance of data delivery in VANETs using 3G. They concluded that due to a centralized authority (Mobile Switching Centre), latency might be an issue as most of the VANET applications are delay-sensitive. With the widespread penetration of 4G networks and the advantages, it offers over 3G in terms of bandwidth, latency, coverage, especially LTE networks. It currently is the most feasible wireless technology suited to implement IoV. Nevertheless, with the advent of 5G in coming years, integration of IoV with 5G networks will have to be accomplished due to the benefits 5G is going to offer over 4G. While integrating IoV with 5G, resource management needs to be accomplished in tandem with user requirements [19].

The increased internet connectivity offered by vehicles has led to challenges in securing the vehicular network as the attack surface area increases [20]. Modern vehicles allow devices to be connected via infotainment systems, creating a pathway to inject malware compromising ECU leading to unforeseen consequences. A framework for vehicular malware characterization and protection has been proposed in [20]. The framework uses virtualization to reduce the vehicular attack surface.

A secure authentication protocol for IoV has been proposed in [21] which mitigates attacks such as offline identity guessing attacks, replay attacks, spoofing and also reduced the authentication time. Although secure, the proposed protocol assumes a secure communication channel between RSU and the TA. The protocol also does away with the usage of passwords as it assumes robust physical vehicular security to prevent theft of smart cards.

Impact of attacks on AODV and GPSR was studied in [22]. Authors simulated attacks on both AODV and GPSR in a vehicular network. Scenarios with high traffic as well as

low traffic density, were considered. It was concluded that AODV is affected more than GPSR by the attacks in a vehicular environment and stressed for the need of security mechanisms in a highly dynamic vehicular environment.

A convolutional network-based Intrusion detection system (IDS)was proposed in [23]. The proposed system is able to intercept and detect network attacks by running on a low powered embedded vehicular terminal by real-time data monitoring.

3 IoV ARCHITECTURE

IoV comprises of a variety of heterogeneous networks and devices communicating with each other. IoV requires a robust architecture that can handle heterogeneity, scalability and various other requirements specific to the IoV paradigm [24]. The general architecture IoV comprises of three layers [25] as depicted in Fig. 1.

Perception/Client Layer comprises of sensors responsible for data gathering, environmental information, location, driving patterns and a lot more. The gathered data collected from the sensors is evaluated/transmitted for further course of action.

The network layer enables communication within vehicular nodes (V2V) and other networks and entities. This layer basically supports all communications within IoV.

The application layer hosts actual applications offered by IoV, manages user interaction, storage, decision making based on data analysis and entertainment and convenience applications such as in-car entertainment, traffic information and much more.

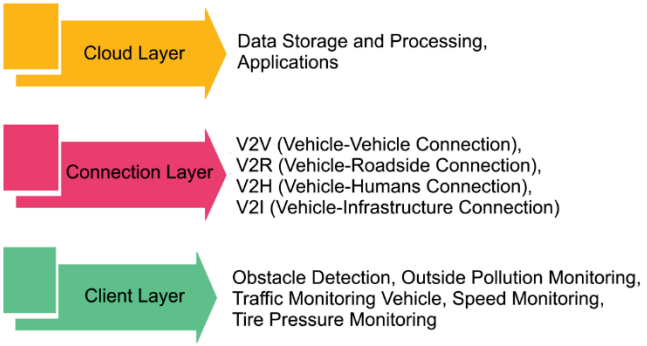

Figure 1 Three-layered IoV architecture.

4 IoV APPLICATIONS

IoV has come up as a very promising paradigm with evolving technology, especially wireless networks and the Internet of Things (IoT). IoV has matured from VANETS to a more significant entity which encapsulates pedestrians, roads, parking lots, city infrastructure, and connects them to provide real-time communication among these entities [26].

IoV provides an extensive and elaborate list of applications [26] which may be broadly grouped as:

- Safety
- Transport Efficiency
- Information/Entertainment/Convenience
- Logistics.

Each of these application categories comprises of multiple applications responsible for enhancing the acceptability of the IoV paradigm; Tab. 2 enlists a few such applications.

Safety in connected vehicles implies that nodes can automatically send real-time crash information, including location information to emergency teams which can expedite the response process and thus help in saving lives.

Cooperative collision warning systems can detect a probable collision and display a warning to the driver to prevent collision [26]. Cooperative forward collision warning systems detect the distance between the cars and alert the driver to prevent rear-end collisions [27]. Driving through an intersection is one of the most challenging tasks a driver faces due to the convergence of multiple traffic streams, thus posing a high possibility of collision [28]. Few approaches have been proposed to avoid collisions at intersections. An abstraction-based algorithm to avoid collisions has been proposed in [29]. An algorithm that can handle a large number of vehicles based on time slots has been proposed in [30]. An intelligent intersection is on the most sought-after safety applications of IoV. Vehicle safety consortium (VSC) has identified some safety-related applications including curve speed warning, pre-crash sensing, cooperative forward collision warning, emergency brake light warning, left turn assistant, traffic signal violation, lane change warning and stop sign movement assistant [26].

Table 2 IoV Applications

Safety	Transport Efficiency	Entertainment /Convenience/ Information
Crash SOS Cooperative Collision Warning Cooperative Forward-Collision Warning Roadside Assistance Left Turn Assistance Lane Change Warning Stop Sign Movement Assistance	Route Guidance and Optimization Green Light Efficiency Traffic Information	Content Streaming Electronic Toll Collection Point of Interest Notification

Some of these applications require Vehicle to Vehicle (V2V) communications while as some require Vehicle to roadside communication (V2R). As such widespread roadside infrastructure for vehicular communication needs to be established in order to implement such safety applications.

Transport efficiency applications such as route guidance and optimization, green light efficiency, can be implemented via IoV. Some of these applications require roadside infrastructure, which some require Vehicle to Vehicle communication only [26]. These applications of IoV

will not only enhance traffic management but will also result in a considerable reduction in journey time, fuel consumption as well as a reduction in pollution levels due to fewer traffic jams. IoV is going to be a key driving force in implementing the smart city concept.

Logistics can benefit from IoV due to its dependence on road transport. Road transportation is essential for timely and efficient delivery of goods. Using IoV in logistics can have far-reaching benefits. IoV can be applied to smart logistics fleet management [31] by a logistic company to improve the delivery of goods. Authors in [31] suggested a smart logistics vehicle management system based on IoV [31]. The primary objective of the proposed system is to equip logistic vehicles with sensors with logistics data control centre as its backbone as visualized in Fig. 2. Working of the proposed system can be explained as follows:

- Logistic vehicles will be equipped with sensors, and these sensors will capture different types of data such as tyre pressure, location, vehicle diagnostics, the status of goods, driving conditions, temperature etc. [31]. A public information centre will provide information such as traffic conditions, weather information and more.
- The goods being transported will be equipped with RFIDs and bar codes that will send data about the goods being carried to the logistics data control centre [31].
- The logistics data control centre will analyze the received data and generate instructions to be sent back based on the result analysis.

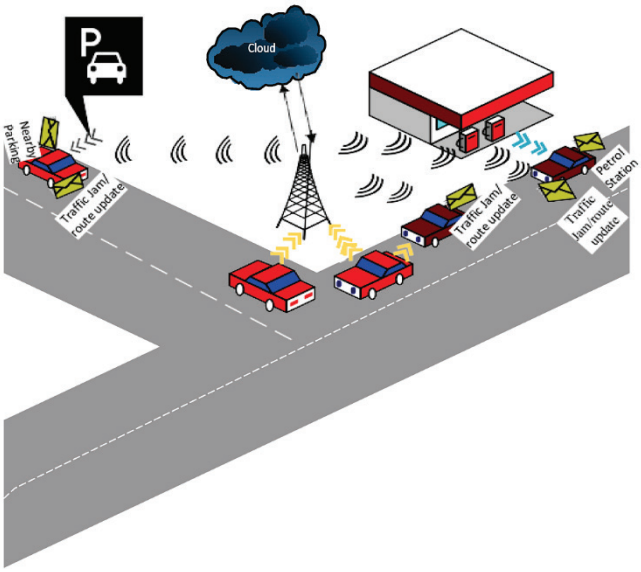

Figure 2 Points of interest and traffic information relayed by nearby roadside units as well as Vehicle-to-Vehicle communication

A prime factor in implementing transport applications in IoV is security and the trust level of the information disseminated. An authentication model for the disseminated information in IoV environment needs to be developed so that bogus and illegitimate information may be stopped from spreading. Bogus information can be detrimental in IoV environment, especially in safety-related applications. Thus, security is a prime concern in IoV and needs further research.

Entertainment/information/convenience include content streaming to in-car entertainment systems, point of interest notifications such as petrol pumps, restaurants, restrooms etc., as represented in Fig. 3. Convenience and entertainment applications range from electronic toll deductions at tolling stations, relay of vehicle diagnostics to the manufacturer for an automated schedule of service, web browsing, streaming to roadside services such as location and price broadcast of fuel stations, parking, restaurants and many more [32].

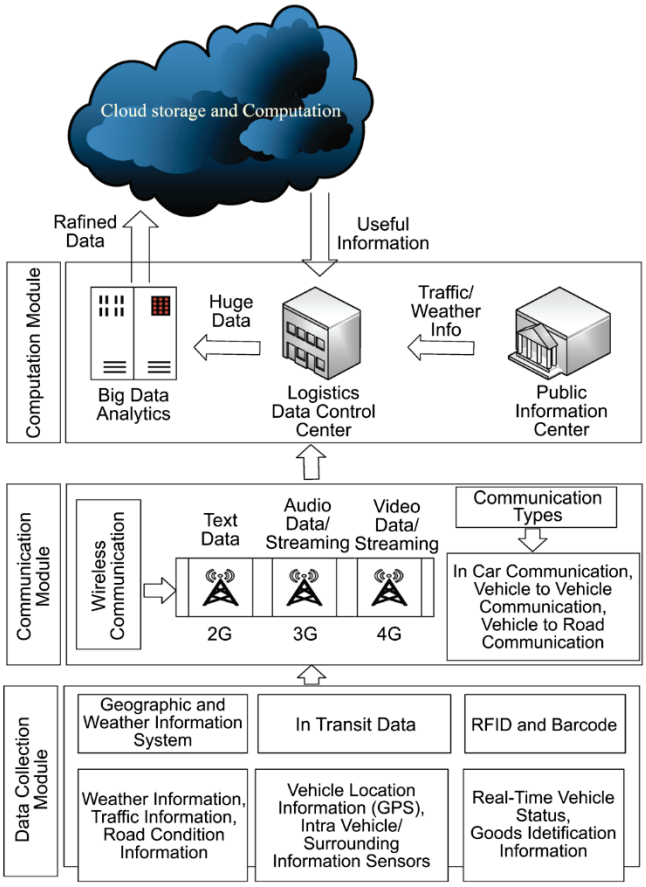

Figure 3 Smart Logistic fleet management system.

5 CHALLENGES

Due to the inherent nature of IoV, it is subject to additional challenges compared to other wireless networks due to its open nature [33]. In IoV no central coordinator can be assumed [26]. Most of the applications are expected to work reliably and efficiently in a decentralized manner [26]. As a result, the need for a single shared channel can be derived. The challenges faced by other wireless networks also inherit themselves into IoV [26], problems faced due to hidden and exposed terminals are evident. Due to the transmission medium being wireless, Medium Access Control (MAC) poses a challenge in the design of VANETs, as many nodes must compete for available channels. The frequency channels assigned to VANET's currently possess bandwidth of 10-20 MHz only. With increasing traffic density and more and more cars being connected, these

channels could choke, causing congestion, posing severe channel management issues [26].

Security is a severe concern in networks, especially wireless networks, and the same applies to VANETs as well [5, 33]. Data integrity, authenticity and trust establishment is a severe issue in vehicular networks [34]. An attacker can fool the network by spreading fake messages [21]. A trust mechanism needs to be established where the receivers are sure enough about the information received. Trust management is a complicated issue in IoV A trade-off must be achieved where users can trust the information without compromising privacy requirements [35]. New paradigms such as Blockchains need to be analyzed for improving user privacy [35, 36, 37]. Achieving a secure communication in IoV is challenging due to a variety of possible attacks [33].

Authors in [38] highlighted attacks that can be carried out in IoV and VANETs. It was concluded that vehicular networks are more susceptible due to their unique characteristics, such as the absence of central authority, mobility, wireless links, cooperativeness, lack of proper lines of defence and scalability [38]. The authors in [38] also proposed defence mechanisms for such attacks but concluded that further research is required With the increasing popularity of autonomous cars, more security issues are creeping [14]. The vulnerability of IoV due to its open nature makes attack detection mandatory [39].

Adoption of VANET equipped vehicles is another issue that needs attention. More and more people must be convinced to buy and use VANET equipped vehicles. The value and benefit provided to a customer in a VANET depend on the total number of customers using VANETs [26] Thus, a key factor is to convince early users to buy VANET equipped vehicles. It can be done by luring customers by offering discounts on VANET equipped vehicles, by installing roadside equipment's for VANETs and enforcement by law. Roadside infrastructure and back end IT connectivity required for VANETs is required to be put in place for smooth and trouble-free deployment.

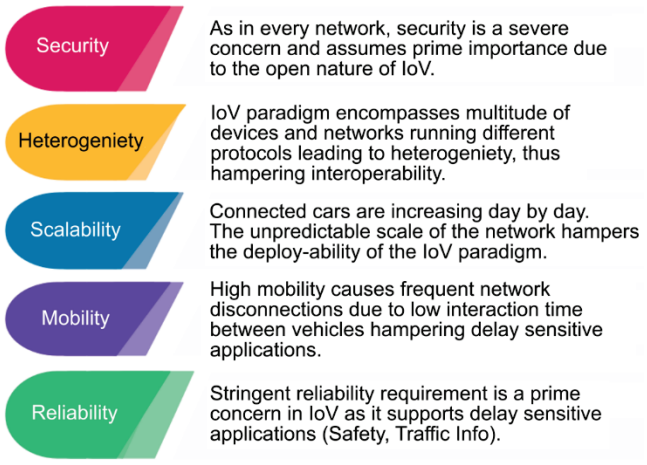

Figure 4 IoV Challenges

The use of cryptographic techniques such as PKI is not particularly suitable for VANETs due issues in key distribution and limited communication time between vehicular nodes [40]. Fig. 4 highlights some of the challenges faced by the IoV paradigm.

6 CONCLUSION

IoV is emerging as a vital component of the smart city concept. It is a unique application of the Internet of Things paradigm. It is a complex network system comprising of heterogeneous devices and networks communicating with each other. As important and beneficial IoV and VANETs are, they have their share of limitations and challenges as discussed. The deploy-ability and rollout of IoV depend on mitigating the issues and challenges faced by these highly dynamic networks. Security and privacy are two factors of utmost importance that need focus. As most of the nodes in a VANET are autonomous, the authenticity and reliability of the disseminated information raise concerns. Trusted communication is the need of the hour as far as VANETs are concerned. A trusted communication can be implemented when a sender is always accepted as a trusted source, and it is made sure that the message in transit has not been tampered with. Thus, security is a prime concern in IoV and VANETs and needs further research. Finally, there are other challenges faced by IoV and VANETs regarding market introduction and demonstration of their capabilities. Efficient methods and policies need to be drafted for the sustainability of services provided as vehicles are introduced as mobile nodes.

Notice

This paper was presented at IC2ST-2021 – International Conference on Convergence of Smart Technologies. This conference was organized in Pune, India by Aspire Research Foundation, January 9-10, 2021. The paper will not be published anywhere else.

7 REFERENCES

[1] Al-Fuqaha, A. et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. *IEEE Communications Surveys & Tutorials. 17. Fourthquarter 2015, 17*(4). https://doi.org/10.1109/COMST.2015.2444095

[2] Alouache, L., Nguyen, N., Aliouat, M., & Chelouah, R. (2018). Survey on IoV routing protocols: Security and network architecture. I*nternational Journal of Communication Systems*, 32. https://doi.org/10.1002/dac.3849

[3] Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wireless Communications and Mobile Computing, Volume 2020*, Article ID 5129620. https://doi.org/10.1155/2020/5129620

[4] Liang, H., Wu, J., Mumtaz, S., Li, J., Lin, X., & Wen, M. (2019). MBID: Micro-Blockchain-Based Geographical Dynamic Intrusion Detection for V2X. *IEEE Commun. Mag., 57*(10), 77-83. https://doi.org/10.1109/MCOM.001.1900143

[5] Sherazi, H. H. R., Iqbal, R., Ahmad, F., Khan, Z. A., & Chaudary, M. H. (2019). DDoS attack detection: A key enabler for sustainable communication in internet of vehicles. *Sustain. Comput. Informatics Syst., 23*, 13-20. https://doi.org/10.1016/j.suscom.2019.05.002

[6] Marquez-Barja, J. M. et al. (2015). Breaking the Vehicular Wireless Communications Barriers: Vertical Handover Techniques for Heterogeneous Networks. *IEEE Transactions on Vehicular Technology, 64*(12), 5878-5890. https://doi.org/10.1109/TVT.2014.2386911

[7] Tornell, S. M., Patra, S., Calafate, C. T., Cano, J.-C., & Manzoni, P. (2015). GRCBox: Extending Smartphone Connectivity in Vehicular Networks. *Int. J. Distrib. Sens. Networks, 11*(3), p. 478064. https://doi.org/10.1155/2015/478064

[8] Wu, W., Yang, Z., & Li, K. (2016). Internet of Vehicles and applications. *Internet of Things: Principles and Paradigm*s, 299-317. https://doi.org/10.1016/B978-0-12-805395-9.00016-2

[9] Sharma, S. & Kaushik, B. (2019). A survey on internet of vehicles: Applications, security issues & solutions. *Vehicular Communications, 20*, 100182. https://doi.org/10.1016/j.vehcom.2019.100182

[10] Sun, Y. et al. (2017). Attacks and countermeasures in the internet of vehicles. *Ann. des Telecommun. Telecommun., 72*(5-6), 283-295. https://doi.org/10.1007/s12243-016-0551-6

[11] Sheikh, M. S., Liang, J., & Wang, W. (2020). Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey. *Wirel. Commun. Mob. Comput., vol. 2020*, 1-25. https://doi.org/10.1155/2020/5129620

[12] Nishiyama, H., Ngo, T., Oiyama, S., & Kato, N. (2015). Relay by Smart Device: Innovative Communications for Efficient Information Sharing among Vehicles and Pedestrians. *IEEE Veh. Technol. Mag., 10*(4), 54-62. https://doi.org/10.1109/MVT.2015.2481558

[13] Dua, A., Kumar, N., & Bawa, S. (2014). A systematic review on routing protocols for Vehicular Ad Hoc Networks. *Vehicular Communications, 1*(1), 33.52. https://doi.org/10.1016/j.vehcom.2014.01.001

[14] Abu Talib, M., Abbas, S., Nasir, Q., & Mowakeh, M. F. (2018). Systematic literature review on Internet-of-Vehicles communication security. *Int. J. Distrib. Sens. Networks, 14*(12). https://doi.org/10.1177/1550147718815054

[15] Wellens, M., Westphal, B., & Mähönen, P. (2007). Performance Evaluation of IEEE 802.11-based WLANs in Vehicular Scenarios. *2007 IEEE 65th Vehicular Technology Conference - VTC2007*, Corpus ID: 7404711. https://doi.org/10.1109/VETECS.2007.247

[16] Yao, Y., Rao, L., Liu, X., & Zhou, X. (2013). Delay analysis and study of IEEE 802.11p based DSRC safety communication in a highway environment. *Proceedings - IEEE INFOCOM*, 1591-1599. https://doi.org/10.1109/INFCOM.2013.6566955

[17] Yang, F., Wang, S., Li, J., Liu, Z., & Sun, Q. (2014). An overview of Internet of Vehicles. *China Commun., 11*(10), 1-15. https://doi.org/10.1109/CC.2014.6969789

[18] Zhao, Q., Zhu, Y., Chen, C., Zhu, H., & Li, B. (2013). When 3G meets VANET: 3G-assisted data delivery in VANETs. *IEEE Sens. J., 13*(10), 3575-3584. https://doi.org/10.1109/JSEN.2013.2265304

[19] Aloqaily, M., Balasubramanian, V., Zaman, F., Al Ridhawi, I., & Jararweh, Y. (2018). Congestion mitigation in densely crowded environments for augmenting QoS in vehicular clouds. *DIVANet 2018 - Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, 49-56. https://doi.org/10.1145/3272036.3272038

[20] Iqbal, S., Haque, A., & Zulkernine, M. (2019). Towards a security architecture for protecting connected vehicles from malware. *IEEE Vehicular Technology Conference, vol. 2019*. https://doi.org/10.1109/VTCSpring.2019.8746516

[21] Chen, C. M., Xiang, B., Liu, Y., & Wang, K. H. (2019). A secure authentication protocol for internet of vehicles. *IEEE Access, 7*, 12047-12057. https://doi.org/10.1109/ACCESS.2019.2891105

[22] Mintemur, O. & Sen, S. (2017). Attack Analysis in Vehicular Ad Hoc Networks. *Computer Science & Information Technology (CS & IT)*, 35-46. https://doi.org/10.5121/csit.2017.71103

[23] Peng, R., Li, W., Yang, T., & Huafeng, K. (2019). An Internet of Vehicles Intrusion Detection System Based on a Convolutional Neural Network. *2019 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Xiamen, China, 1595-1599. https://doi.org/10.1109/ISPA-BDCloud-SustainCom-SocialCom48970.2019.00234

[24] Tuyisenge, L., Ayaida, M., Tohme, S., & Afilal, L.-E. (2018). Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues. In: Skulimowski A., Sheng Z., Khemiri-Kallel S., Cérin C., Hsu CH. (eds) *Internet of Vehicles. Technologies and Services Towards Smart City. IOV 2018. Lecture Notes in Computer Science, vol 11253*. Springer, Cham. https://doi.org/10.1007/978-3-030-05081-8_1

[25] Huang, J. M. (2013). Research on Internet of Vehicles and its Application in Intelligent Transportation. *Applied Mechanics and Materials*, 321-324, 2818-2821. https://doi.org/10.4028/www.scientific.net/AMM.321-324.2818

[26] Hartenstein, H. & Laberteaux, K. P. (2008). A tutorial survey on vehicular ad hoc networks. *IEEE Communications Magazine, 46*(6), 164-171. https://doi.org/10.1109/MCOM.2008.4539481

[27] Kowshik, H., Caveney, D., & Kumar, P. R. (2011). Provable systemwide safety in intelligent intersections. *IEEE Trans. Veh. Technol., 60*(3), 804-818. https://doi.org/10.1109/TVT.2011.2107584

[28] Toor, Y., Mühlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. *IEEE Commun. Surv. Tutorials, 10*(3), 74-88. https://doi.org/10.1109/COMST.2008.4625806

[29] Colombo, A. & Del Vecchio, D. (2011). Supervisory control of differentially flat systems based on abstraction. *Proceedings of the IEEE Conference on Decision and Control*, 6134-6139. https://doi.org/10.1109/CDC.2011.6160759

[30] Colombo, A. & Del Vecchio, D. (2012). Efficient algorithms for collision avoidance at intersections. *HSCC'12 - Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control*, 145-154. https://doi.org/10.1145/2185632.2185656

[31] Sharma, N., Chauhan, N., & Chand, N. (2016). Smart logistics vehicle management system based on internet of vehicles. *The 4th International Conference on Parallel, Distributed and Grid Computing, PDGC 2016*, 495-499. https://doi.org/10.1109/PDGC.2016.7913245

[32] Hossain, E. et al. (2010). Vehicular telematics over heterogeneous wireless networks: A survey. *Comput. Commun., 33*(7), 775-793. https://doi.org/10.1016/j.comcom.2009.12.010

[33] Raya, M. & Hubaux, J. P. (2007). Securing vehicular ad hoc networks. *J. Comput. Secur., 15*(1), 39-68. https://doi.org/10.3233/JCS-2007-15103

[34] Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., & Park, Y. (2020). Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges. *IEEE Access, 8*, 54314-54344. https://doi.org/10.1109/ACCESS.2020.2981397

[35] Butt, T., Iqbal, R., Salah, K., Aloqaily, M., & Jararweh, Y. (2019). Privacy management in social internet of vehicles: Review, challenges and blockchain based solutions. *IEEE Access, 7*, 79694-79713. https://doi.org/10.1109/ACCESS.2019.2922236

[36] Taiyaba, M., Akbar, M. A., Qureshi, B., Shafiq, M., Hamza, H., & Riaz, T. (2020). Secure V2X Environment using Blockchain Technology. *EASE '20: Proceedings of the Evaluation and Assessment in Software Engineering*, 469-474. https://doi.org/10.1145/3383219.3383287

[37] Ramaguru, R. B., Sindhu, M., & Sethumadhavan, M. (2019). Blockchain for the Internet of Vehicles. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Kashyap R. (eds) Advances in Computing and Data Sciences. *ICACDS 2019. Communications in Computer and Information Science, vol 1045*. Springer, Singapore. https://doi.org/10.1007/978-981-13-9939-8_37

[38] Sakiz, F. & Sen, S. (2017). A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV. *Ad Hoc Networks, 2017.* https://doi.org/10.1016/j.adhoc.2017.03.006

[39] Hasan, M., Mohan, S., Shimizu, T., & Lu, H. (2020). Securing Vehicle-to-Everything (V2X) communication platforms. *IEEE Transactions on Intelligent Vehicles, 5*(4), 693-713. https://doi.org/10.1109/TIV.2020.2987430

[40] Malhi, A. K., Batra, S., & Pannu, H. S. (2020). Security of vehicular ad-hoc networks: A comprehensive survey. *Comput. Secur., 89*, p. 101664. https://doi.org/10.1016/j.cose.2019.101664

Authors' contacts:

Faisal Rasheed Lone
(Corresonding author)
BGSB University,
National Highway Road 144A, Dhanore,
Rajouri, Jammu and Kashmir 185234, India
fasulone@gmail.com

Harsh Kumar Verma
NIT Jalandhar,
GT Road Byepass, NH-1,
Jalandhar 144011, Punjab, India
vermah@nitj.ac.in

Krishna Pal Sharma
NIT Jalandhar,
GT Road Byepass, NH-1,
Jalandhar 144011, Punjab, India
sharmakp@nitj.ac.in