# Analysis of Various Techniques of Internet of Vehicles

**Sonali Gupta**, **Manika Manwal**, **Manisha Aeri**

***Abstract :The vehicular ad hoc network is the network in which vehicles can move from one location to another without help of driver. The vehicle ad hoc network has two type of communication which is vehicles to vehicle and vehicle to road side units. The internet of things is the technology in which source can transmit sensed information over the internet. This research work is based on the vehicle of internet things. In the vehicles of internet things, the vehicles are connected with each other through internet. The various techniques of data aggregation in vehicle of things are reviewed in this paper and analyzed in terms of certain parameters***

***Keywords: VANET, IoT, Data Aggregation, IoV***

## I. INTRODUCTION

The network that extends as well as expands on the Internet is known as Internet of Things (IoT). The wireless sensors and intelligent network systems are the core of this network design. For identifying and exchanging the data through radio frequency identification (RFID) and using human-machine dialogue to transmit he collected information to wireless LAN, the sensors are deployed among the objects or people and objects by IoT networks. The monitoring, management, location, and tracking of data are possible through this network [1]. A larger network is formed by IoT by connecting all kinds of things around the people with Internet. The information can be extracted and processed rapidly through this network. An unprecedented convenience is provided to life and production through the rational use of this information. For realizing the real-time information exchange, the vehicle is linked with the infrastructure of vehicle and the roadside through Internet of Vehicles (IoV). In the transportation network, this is the specific application of Internet of Things. To ensure that the static and dynamic information of all vehicles is extracted and used on information network platform in effective manner, the wireless communication is provided by IoV. The functional requirements are used to effectively surprise the vehicles and comprehensive services are provided by them [2]. Vehicle network helps in collecting, distributing and processing the data dynamically through IoV and the information is shared using wireless communication such that the information among vehicle and existing network can be exchanged. The vehicle can be linked to city network as a result of this.

**Revised Manuscript Received on May 07, 2020.**
**Sonali Gupta**, Assistant Professor, Graphic Era Hill University,Dehradun (U.K) m.sonaligupta15@gmail.com
**Manika Manwal**, Assistant Professor, Graphic Era Hill University,Dehradun (U.K) manikamanwal17@gmail.com
**Manisha Aeri**, Assistant Professor Graphic Era Hill University,Dehradun (U.K) maniaeri16@gmail.com

The global satellite positioning systems and wireless communication technologies are linked to design the in-vehicle intelligent communication service provided in IoV. There is the vehicle position, driving speed and driving route included in an information interaction network [3]. The electronic devices are used to collect information from various objects or devices. For realizing intelligent monitoring, scheduling and management of people, roads and vehicles, the computer technology is used by cloud center which helps in analyzing and processing the collected information. Simultaneously, the traffic information and real-time navigation services can be attained by the driver by contacting the center at any time using wireless signals. A special mobile wireless sensor network is designed by IoV using the vehicles as carriers. Vehicle area network (VAN) and vehicular Ad Hoc network (VANET) are the two different types of networks. A local area network built within the vehicle and helps in exchanging information among the vehicle sensor, communication and positioning modules is known as VAN. A mobile self-configuring type of network designed for traffic environments in known as VANET [4].

### 1.1 Security in IoV

The IoV networks face several security related challenges since they are self-configuring in nature and are linked directly with internet. The topology of these networks is also dynamic since the deployed devices are mobile. The vulnerability of nodes to the external threats is high due to the internet connectivity. Any kind of malicious activity can be performed by unauthorized users based on the information provided by the nodes. Thus, catastrophic outcomes such as accidents can occur as a result of interruptions by the malicious users. Thus, the security of complete network is compromised here. Since the human lives are at risk in such networks, it is important to ensure the security of IoV networks. Due to the distinctive properties of IoV, several security-related challenges are being faced in these networks. Security challenges like trust group formation, certificate management, position detection and data protection are faced due to the unique properties of these networks [5].

### 1.2 Security schemes for IoV network

There are, encryption and trust based security techniques designed to secure the IoV networks which are explained below:

a. Encryption based schemes: They are of 2 types which are symmetric encryption scheme (SES) and public-key encryption scheme (PES). The encryption and decryption methods use single key in SES techniques. However, a different key is used for encryption and decryption in case of PES.

The advantage of computational complexity is provided through SES. In comparison to PES, the encryption speed of SESs is higher since they provide less computational complexity [6].

b. Trust based schemes: The soft security measures that completely rely on the behavior of nodes are handled through trust based schemes. These security methods are highly suitable for securing IoV networks since the security of data completely depends on the trustworthiness of nodes.

## II. LITERATURE REVIEW

Sunil Kumar, et.al (2019) proposed a machine learning based Delimitated Anti Jamming protocol that was applicable in vehicular traffic scenarios [7]. With the aim of knowing the precise location of jamming effected vehicles, the discriminated signal of jamming vehicle is detected and filtered. Specifically, with focus on the localization of vehicles in the delimitated jamming scenarios, this research proposed a vehicular jamming system model. The traditional approaches and the proposed anti jammer approach were compared to evaluate the performance. Based on the various performance parameters, the proposed approach attested to outperform existing approaches.

Liangmin Wang, et.al (2018) studied the threats caused by multiple networks access and fusion for actual vehicles and also presented an attack model [8]. Further, based on the assessment of security levels and threats, the NOTSA was proposed. The security proofs were then used to analyze the security of proposed method. RBD and formula analysis were used to analyze the reliability of this approach. For evaluating the performance and security, a hardware experimental scenario was constructed in the simulation and evaluation. Additionally, MATLAB was applied for evaluating the reliability of RSU, communication networks and NOTSA. The feasibility and efficiency of proposed method were proved through the achieved outcomes. This research could be extended in future to improve the reliability, performance and level of security of proposed technique.

Nishant Sharma, et.al (2018) studied the various security based issues being faced in IoV along with its development [9]. To ensure a secure communication among two nodes present in IoV, an authentication approach was proposed. To ensure that no malicious node intruded the working of system, this approach was used. The public key infrastructure cryptography technique helped in authenticating both base station and the vehicle to IoV network using this proposed method.

Yongfeng Qian, et.al (2018) proposed a path selection mechanism to secure the CIoV systems, through which the rules of delay-sensitive traffic were forwarded [10]. The path selection strategy used here was described using the 0-1 programming problem. The problem was transformed into convex optimization issue as a solution. The research experiments conducted showed that in terms of average transmission delay and end-to-end transmission delay, the performance of proposed method was better as compared to general IoV.

Danda B. Rawat, et.al (2017) described data falsification intrusion with hashes [11]. The main aim here was to improve the security and efficiency of network by adjusting the magnitude of contention window so that the accurate data could be transferred to the adjoining vehicles in proper time. This work also made use of a clustering algorithm for reducing travel time during traffic jam. The mathematical outcomes obtained from simulations were used in this work for evaluating the efficiency of recommended scheme. It was analyzed that recommended flexible algorithm prevented data falsification intrusions in Internet of Vehicles. This algorithm provided better throughput with lower delay than other existing algorithms.

Longhua Guo, et.al (2017) presented a secure approach for collecting massive volume of data in big scale IoV to improve its functioning in terms of security and efficacy [12]. A first, it was required to register vehicles in the large data hub for establishing their connection with the network. Then, this work used mutual verification and sole sign-on algorithm for connecting vehicles with large data hub. In this work, two dissimilar secure protocols were presented for collecting commercial and private data. The storage of gathered data was carried out in secured manner with distributed storage. The achieved outcomes demonstrated that the recommended approach was quite secure and efficient.

Hsin-Te Wu, et.al (2017) recommended a new approach emphasizing the use of road side units for evaluating the traffic flow and helping emergency vehicles [13]. The use of road side units for controlling traffic signals during traffic jam could enhance the rescue efficacy of emergency vehicles. The vehicles on the road could face any event. In these conditions, the vehicles could use recommended approach for obtaining GPS information from law enforcement agencies as an evidence of event. On the other hand, law enforcement agencies could get visual evidence of serious accidents from other vehicles. It was required for the recommended approach to be based on the network security for ensuring the genuineness of the information. Also, the tested outcomes revealed that the recommended approach performed better than earlier approaches. The future work would continue the use of this approach and try to find a new way to fulfill the different needs without being based on roadside units.

**Table 1: Comparison Table**

| Author | Year | Description | Outcomes | Future scope |
|---|---|---|---|---|
| Sunil Kumar, Karan Singh, Sushil Kumar, Omprakash Kaiwartya, Yue Cao, Huan Zhou | 2019 | Proposed a machine learning based Delimitated Anti Jamming protocol that was applicable in vehicular traffic scenarios. | Based on the various performance parameters, the proposed approach attested to outperform existing approaches. | The future work would be focused on the development of more approaches for ensuring security in IoV. |
| Liangmin Wang, Xiaolong Liu | 2018 | Studied the threats caused by multiple networks access and fusion for actual vehicles and also presented an attack model. Further, based on the assessment of security levels and threats, the NOTSA was proposed. | The feasibility and efficiency of proposed method were proved through the achieved outcomes. | This research could be extended in future to improve the reliability, performance and level of security of proposed technique. |
| Nishant Sharma, Naveen Chauhan, Narottam Chand | 2018 | Studied the various security based issues being faced in IoV along with its development. To ensure a secure communication among two nodes present in IoV, an authentication approach was proposed. | The public key infrastructure cryptography technique helped in authenticating both base station and the vehicle to IoV network using this proposed method. | The future work would be focused on addressing other challenges in IoV other than security. |
| Yongfeng Qian, Min Chen, Jing Chen, M. Shamim Hossain, Atif Alamri | 2018 | Proposed a path selection mechanism to secure the CIoV systems, through which the rules of delay-sensitive traffic were forwarded. | The research experiments conducted showed that in terms of average transmission delay and end-to-end transmission delay, the performance of proposed method was better as compared to general IoV. | The future work would be focused on the development of more approaches for ensuring security in IoV. |
| Danda B. Rawat, Moses Garuba, Lei Chen, Qing Yang | 2017 | Described data falsification intrusion with hashes. The main aim here was to improve the security and efficiency of network by adjusting the magnitude of contention window so that the accurate data could be transferred to the adjoining vehicles in proper time. | It was analyzed that recommended flexible algorithm prevented data falsification intrusions in Internet of Vehicles. This algorithm provided better throughput with lower delay than other existing algorithms. | The future work would be focused on integrating the existing IoV security tools. |
| Longhua Guo, Mianxiong Dong, Kaoru Ota, Qiang Li, Tianpeng Ye, Jun Wu, Jianhua Li | 2017 | Presented a secure approach for collecting massive volume of data in big scale IoV to improve its functioning in terms of security and efficacy. | The storage of gathered data was carried out in secured manner with distributed storage. The achieved outcomes demonstrated that the recommended approach was quite secure and efficient. | The future work would be focused on doing some further research regarding the routing protocol of IoV for optimizing the recommended security mechanism. |

| | | | | |
|---|---|---|---|---|
| Hsin-Te Wu, Gwo-Jiun Horng | 2017 | Recommended a new approach emphasizing the use of road side units for evaluating the traffic flow and helping emergency vehicles. | The use of road side units for controlling traffic signals during traffic jam could enhance the rescue efficacy of emergency vehicles. | The future work would continue the use of this approach and try to find a new way to fulfill the different needs without being based on roadside units. |

## III. CONCLUSION

In this paper, it is concluded that vehicular ad hoc network and internet of things are joined together to form vehicle of internet technology. In the internet of things technology, the sensed data can be transmitted through the internet with each other. The vehicular ad hoc internet is the technology in which vehicles can share the information with each other through the internet. In this paper, various techniques of IoV are reviewed in terms of certain parameters.

## REFERENCES


1. Abdus Samad, Shadab Alam, Mohammed Shuaib, "Internet of Vehicles (IoV) Requirements, Attacks and Countermeasures", 2018, 5th International Conference on "Computing for Sustainable Global Development
2. Surbhi Sharma, Baijnath Kaushik, "A survey on internet of vehicles: Applications, security issues & solutions", Vehicular Communications, Volume 20, December 2019, Article 100182
3. Shushu Liu, An Liu, Zheng Yan, Wei Feng, "Efficient LBS queries with mutual privacy preservation in IoV", Vehicular Communications, Volume 16, April 2019, Pages 62-71
4. Yunchuan Sun, Lei Wu, Shizhong Wu, Shoupeng Li, Tao Zhang , Li Zhang, Junfeng Xu, Yongping Xiong, "Security and Privacy in the Internet of Vehicles", 2015, International Conference on Identification, Information, and Knowledge in the Internet of Things (IIKI)
5. Indu Bhardwaj, Sibaram Khara, "Research trends in Architecture, Security, Services and Applications of Internet of Vehicles (IOV)", 2018, International Conference on Computing, Power and Communication Technologies (GUCON)
6. Lata Yadav, Sudhanshu Kumar, Anil KumarSagar, Subrata Sahana, "Architechture, Applications and Security for IOV: A Survey", 2018, International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)
7. Sunil Kumar, Karan Singh, Sushil Kumar, Omprakash Kaiwartya, Yue Cao, Huan Zhou, "Delimitated Anti Jammer Scheme for Internet of Vehicle: Machine Learning Based Security Approach", IEEE Access, 2019, Volume: 7
8. Liangmin Wang, Xiaolong Liu, "NOTSA: Novel OBU With Three-Level Security Architecture for Internet of Vehicles", IEEE Internet of Things Journal, 2018, Volume: 5, Issue: 5
9. Nishant Sharma, Naveen Chauhan, Narottam Chand, "Security challenges in Internet of Vehicles (IoV) environment". 2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)
10. Yongfeng Qian, Min Chen, Jing Chen, M. Shamim Hossain, Atif Alamri, "Secure Enforcement in Cognitive Internet of Vehicles", IEEE Internet of Things Journal, 2018, Volume: 5, Issue: 2
11. Danda B. Rawat, Moses Garuba, Lei Chen, Qing Yang, "On the security of information dissemination in the Internet-of-Vehicles", Tsinghua Science and Technology, 2017, Volume: 22, Issue: 4
12. Longhua Guo, Mianxiong Dong, Kaoru Ota, Qiang Li, Tianpeng Ye, Jun Wu, Jianhua Li, "A Secure Mechanism for Big Data Collection in Large Scale Internet of Vehicle", IEEE Internet of Things Journal, 2017, Volume: 4, Issue: 2
13. Hsin-Te Wu, Gwo-Jiun Horng, "Establishing an Intelligent Transportation System with a Network Security Mechanism in an Internet of Vehicle Environment", IEEE Access, 2017, Volume: 5