Journal of Harbin Engineering University
ISSN: 1006-7043

Vol 44 No. 7
July 2023

Investigation on a wide variety of threats and protective measures for the VANET

Ms Shubhra Mukherjee [1]*, Dr Ravindra Gupta [2]

[1]Sarvepalli Radhakrishnan University, India
[2]Sarvepalli Radhakrishnan University, India, mukherjeeshubhra@gmail.com

Abstract-Vehicular network is a kind of dynamic network where vehicles move freely in defined road map. In the VANET road side unit (RSU) play the important role to controlling and monitoring the vehicles in the network, every vehicles under the surveillance of RSU because in the dynamic network trust reputation is very poor between vehicles. In the new era of technology vehicular communication provide real time information of road information i.e. warning message, accidental information, congestion etc. To adaptability of VANET in real time scenario having some hurdles such as poor network connectivity, security challenges and dynamic network (frequently changes topology). In this paper investigate the security challenges, different types of attack and their prevention mechanism for vehicular communication. The dynamic network is highly vulnerable network because number of mis-activity exist in the network during communication i.e. data gathering by malicious users, grayhole, blackhole, route capturing, denial of service, Sybil attack etc. The investigation of attack and security measures shows that some of attack easy way to detect and prevent by various security techniques. But some of attacks is easily not detected because topology of VANET are frequently changes the position of vehicle which creates hurdle to get complete information of attacker node in real time. To increasing the security of VANET it's require depth behaviour analysis of attacks and apply classify proper attack with its preventive measures. In future implement security system using vehicle location, depth behaviour analysis, activity analysis and vehicle identity based attack detection system and collaborative security system for VANET network.

Keywords-VANET, RSU, Sybil attack, authentication, security..

Introduction

A vehicular ad hoc network (VANET) is a kind of mobile ad hoc network (MANET) that enables wireless communication between moving vehicles. This is a fully decentralised and self-managing communication infrastructure. Nodes in a VANET act as both servers and clients, passing and receiving data between them. New transportation technologies are expected to provide passengers with a variety of amenities, such as safety apps, driving assistance, emergency notifications, etc. To improve road safety through coordinated transportation, MANETs have been adapted to function as vehicular ad hoc networks (VANETs). However, there is something that may endanger the car and its occupants: the vehicle could be followed, traced, or have its communications spied upon. The vehicular ad hoc network (VANET) is a special type of MANET. Recently, VANETs have been developed to accommodate the proliferation of wireless gadgets suitable for usage in automobiles [1]. GPS devices, cell phones, and laptop computers are just a few examples. In contrast to MANETs, VANETs contain features like unlimited energy, no fixed network size, a dynamic topology, mobility models, no fixed nodes, and precise location. Due to these factors, efficient routing protocols were difficult to create in the VANET environment. The primary contributors are the frequently relocating mobile nodes.

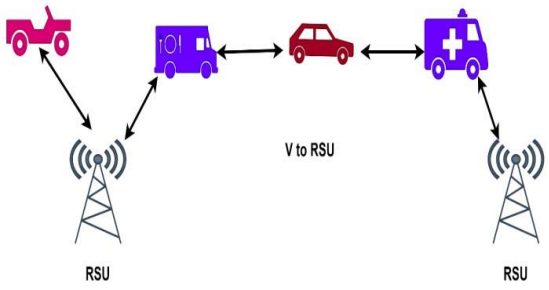

Figure 1: Vehicle to RSU Communication

There are more traffic accidents, fatalities, and injuries as a result of people travelling more

often, which comes at a high cost to society. Supporting services for Intelligent Transportation Systems (ITSs) are envisioned to be provided through Vehicular AdHoc Networks (VANETs), such as collective traffic monitoring, collision avoidance, vehicle navigation, control of traffic signals, and signalling to drivers to alleviate traffic congestion. Vehicle-to-vehicle and vehicle-to-roadside equipment networks (VANETs) provide wireless and multi-hop communication between moving and stationary network nodes. We expect that VANET security will help us accomplish our goals [2]. It needs to guarantee the correctness of the data received (information authenticity), the integrity and veracity of the messages sent and received, the anonymity of the node sending the message (privacy), and the sturdiness of the system overall.

VANET Characteristics

A vehicle ad hoc network has its own distinct traits that set it apart from other kinds of mobile ad hoc networks. The unique characteristics of a VANET provide the potential to boost network performance while also posing significant hurdles. When compared to other MANETs, a VANET has significant differences [4].

High Mobility: The nodes in VANETs are often very mobile, moving at rapid speeds. The protection of node privacy is enhanced, and it becomes more difficult to guess a node's location.

Rapidly changing network topology: Due to the variable speeds of cars and the great mobility of nodes, the network's topology is constantly shifting. Because of this, the structure of VANET networks is dynamic.

Unbounded network size: Scalability to any size network, from a single city to a national network. This means there is no physical limit to the scale of a VANET network.

Types of Attack in VANET

Regular information sharing: The decentralised structure of VANET encourages nodes to actively seek out data from other cars and infrastructure components. As a result, communication between nodes increases in frequency.

The use of vehicular ad hoc networks (VANET) has the potential to greatly enhance road safety and passenger convenience. However, as they rely on open means of communication, they are vulnerable to a variety of attacks that might compromise their security. The importance of security and privacy characteristics in VANET networks, which will be described in this title [3], cannot be overstated. In this study, we look at the mechanisms that help avoid assaults and ensure the VANET can communicate safely. The current setup is useful for determining what has to be studied in order to improve the security of automotive ad hoc networks against Sybil attacks. The vehicle ad hoc network (VANET) is one such technology that will soon be put into us.

Wireless Communication: VANET is built for a wireless network topology; hence, its communications are wireless as well. Information is shared between nodes and sent wirelessly. As a result, it's important to think about how to keep our conversations safe

Time-sensitive: in a VANET, data must reach nodes quickly enough for them to make a judgement and take appropriate action before the deadline passes. Sufficient Energy: The VANET nodes have plenty of power and computing capacity, so that's not an issue. This not only provides infinite transmission power but also enables sophisticated techniques like Rivest Shamir Adleman (RSA) and the Elliptic Curve Digital Signature Algorithm (ECDSA) to be used in VANETs.

The role attacker is only to disturb the normal functioning of network. There are different types of attacks in VANET [1][5][6]. The attackers are External and Internal it’s depends on the presence of attacker inside or outside the network. The attackers are active type and passive type, it’s depending on the attacker malicious behavior. The some of the harmful attacks on MANET are: -

Sybil Attack

A Sybil attack is one in which the malicious node masquerades as many nodes. This form of assault makes an effort to lessen the workload

placed on the distributed algorithms that are in use and, as a consequence, their level of success. Sybil attacks are undertaken often against distributed storage, routing, data aggregation, voting, fair resource allocation, and mischief detection. [Sybil] is an acronym for "Sybil Attacks."

Wormhole Attack

A wormhole attack is an attack in which a malicious node tunnels messages from one portion of the network to another via a link that does not ordinarily exist. This allows the attacker to bypass security measures that would normally prevent such an attack. The only sort of wormhole attack is one in which two nodes are tricked into believing that they are neighbors to one other. This attack would probably certainly be implemented in tandem with selective forwarding or listening in on conversations.

Sinkhole Attack

In a sinkhole attack, the goal of the attacker is to divert all traffic through their exploit. When a protocol is built on flooding, for example, a hacked node may receive route requests and then respond to the node that asked for them with messages that avoid a false route and offer the quickest way to the destination that is wanted.

Falsified, Modified, or Replayed Routing Information.

As the data is being transmitted, it is possible for it to be falsified, changed, replayed, or destroyed. Because the sensor nodes only transmit over a small distance, it is possible for an adversary with a considerable amount of processing power and a longer communication range to attack multiple sensors at the same time and alter the data that is being delivered.

Forwarding with Selectivity

One form of forwarding is known as selective forwarding, and it gives users the ability to choose the content that is forwarded. As part of this plausible form of attack, a rogue node may act as a region by declining to forward every message it receives, or alternatively, it may selectively forward some messages to the incorrect target while discarding others.

Literature Review

S. No.	Title of the Paper	Author/Year/Journal/ Conference	Work Done In the Paper	Improvement needs
1	Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance	Nirbhay Kumar Chaubey, Dhananjay Yadav, 2022, International Journal of Electrical and Computer Engineering (IJECE) [7].	Proposed scheme for Sybil attacker. First forecasting the number of vehicles on the road and then assessing network performance by computing the packet delivery ratio (PDR) in the network. PDR is affected by a variety of factors, including transmission power, actual physical phenomena, and topological changes caused by high vehicle speeds. Because RSU is always placed alongside the road, its transmission power and physical	Sybil attack behavior classification and their analysis not done. In future improvement require to analysis two type of Sybil attack detection and prevention with their impact into the network.
			phenomena are fixed, and it has minimal impact on PDR calculation.	

2	Sybil attack's impact on VANET's Authentication Service	Mustafa Maad Hamdi, Al-Maarif Sami Abduljabbar Rashid, Majeed Dhafer, Ahmed Jamal Ahmed , Ahmed Shamil Mustafa Ahmed Muhi Shantaf, 2022, IEEE International Congress on HumanComputer Interaction, Optimization and Robotic Applications (HORA) [8].	The Sybil attack is introduced after a discussion of criteria and the most recent developments in this study. An adversary may employ a sybil assault by pretending to be several people at once. Consideration must also be given to the delay in receiving messages across the VANET. Data sharing security is critical in VANET because any traffic accident could be disastrous. Where, VANET developers confront a number of obstacles. Problems might arise while trying to decide on a suitable architecture or when trying to set up a reliable connection to a VANET. Due to the high speeds at which the vehicles are travelling, effective communication is challenging. Data integrity and defense against new security threats are two additional major issues. A sybil attack is one in which an attacker uses many identities to simulate heavy traffic.	In this paper authentication based Sybil attack is detected which require further improvement of detection scheme under dynamic behavior using distributed security technique. In future distributed security scheme increases the accuracy for attack detection.
3	Protecting V-RSU Communications on VANET against Blackhole and Wormhole Attacks with an Intrusion Prevention System	Gaurav Soni, Kamlesh Chandravanshi, M.K Jhariya, Arjun Rajput, 2022, Contemporary Issues in Communication , Cloud and Big Data Analytics [9].	Proposed Privacy-preserving under Denser Traffic Management (PPDM) schemes against blackhole attacker that damaging network behaviour. Without security guarantees, some disobedient or malicious cars make the system vulnerable to providing low-quality services or even putting user vehicles in dangerous situations in 6G-VANET. As a result, detecting misbehaving or malicious cars has evolved into a vital challenge in VANET security. The security mechanism for locating an attacker's car is based on network traffic statistics. The system detects the attacker's presence and estimates the total number of packets lost in the network by the blackhole attacker.	In this article detect and prevent the blackhole and wormhole attack in VANET using RSU based monitoring method in future need to secure VANET from different attacks i.e. DoS, Sybil and jamming attacks.
4	A Novel Privacy-Preserving and Denser Traffic Management System in 6GVANET Routing Against Black Hole Attack	Gaurav Soni, Kamlesh Chandravanshi, 2022, Sustainable Communication Networks and Application(ICS CN21) [10].	Proposed Intrusion Detection and Prevention (IPS) scheme with PSO in VANET. The intelligence of the swarm provides information about the existence of the attacker and also determines the secure path for routing between sender and receiver in the network. Higher pheromone values in the network are used to choose routes. In order to guarantee safety and alert all parked RSUs and vehicles in the vicinity about the attacker's vehicle, the PSO	In this research article they use the concept of swarm optimization for enhancing 6G-VANET communication and security measures that work further need to improve while applying location sensing technique or signal

			technique for V-to-RSU communication is provided here. The proposed preventative method is an attempt to stop cybercriminals and guarantee a safe connection on VANET.	strength to increase reliability.
5	Prevention of Denial-of-Service Attack Over Vehicle Ad hoc Networks using Quick Response Table	Paramjit Singh Waraich, Neera Batra, 2017, IEEE4th International Conference on Signal Processing, Computing and Control (ISPCC) [11].	Proposed a scheme to secure the VANET from DoS, using Quick Response Tables (QRT) which can analyze the frequent updates in routing information and uses a reference table. If any node acts as an intruder, then its status is saved in QRT table for future use. Finally, all nodes are informed about this Log and it is further used for route maintenance to avoid the entries of malicious nodes. Security analysis shows that packet drop at earlier stages is considered as normal packet drop but at a later stage, on the basis of QRT Logs, large scale packet drop can be identified easily, thus resulting in the isolation of intruder from routing table. QRT maintains a reference of each event at current routing path and once a Log for a specific node is created, identified node is ignored by neighbors and finally, QRT prevents the entire network from DoS attack.	In this paper secure the VANET network from denial of service attack using QRT response table but in the dynamic network, multiple attacks exist. To secure the complete network from all types of attack need some distributed security techniques to handle various mis-activity by groups of VANET as per attack activity.
6	Techniques for Key Management and Dual Authentication in Vehicular Ad Hoc Networks for Secure Data Transmission	Shamuyarira K and Saraswathi K, 2017, International Journal of Recent Scientific Research [12].	The major goal of this title is to enhance the safety of VANETs by facilitating faster decision-making and more reliable communication through authentication. Personal information of the user, such as his or her identity and location, may be used for authentication. A VANET system primarily improves the level of confidentiality. Dual authentications give a high level of vehicleside security to prevent unauthorized vehicles from entering the VANET. To prevent unauthorised parties from discovering where vehicles are parked, the Hierarchical Privacy Preserving Pseudonym Authentication Protocol was developed.	In this article, they secure the VANET using dual authentication and key management techniques, which require some static centralized monitoring systems. In the future, authentication systems will adopt dynamic networks to secure VANET, which provide flexible security and control systems and more realistic adaptability.

7	Effective Multichannel Medium Access Control (MAC) Protocol for Mobile Ad Hoc Networks with Quality of Service Support	Caixia Song, Guozhen Tan and Chao Yu, 2017, mdpi Sensors [13].	Designed a multichannel medium access control (MAC) protocol for vehicular ad hoc networks that is both efficient and supports quality of service. In this research, we focus on a protocol for highway-based VANETs called Efficient and QoS-Supported Multichannel Medium Access Control (EQMMAC). The EQM-MAC protocol uses the service channel resources for non-safety message transmissions during the whole synchronization interval, and it adapts the minimum contention window size for various non-safety services in real time according to the load. High saturation throughput and low transmission latency may be maintained by using the EQM-MAC protocol, according to a theoretical model study and extensive simulation findings.	In this article, they improve VANET performance using the multichannel MAC protocol. It is also required to secure the network from different attacks and maintain the QoS of VANET.
8	Performance Comparison between Broadcast Authentication Methods for Vehicular Networks	Kanika Grover, Alvin Lim, 2016, ICINS [14].	In this title, we compare the performance of broadcast authentication methods for vehicular networks. The Elliptic Curve Digital Signature Algorithm (ECDSA) is a recommended method of authentication for time-sensitive broadcast messages in the IEEE 1609.2 standard for VANETs. Although ECDSA verification is costly in terms of time, TESLA and signature amortization are the algorithms most frequently recommended as alternatives. Sadly, neither immediate authentication nor non-repudiation are present in these algorithms. In light of this, To authenticate using ECDSA, we introduce a probabilistic verification strategy. Using NS2 simulation tools, we evaluate the efficacy of the aforementioned broadcast authentication methods.	In this article, they secure vehicular networks using a digital signature-based authentication system. It requires further improvement of the security system to protect data from network layer attacks, i.e., blackhole, wormhole, or grayhole attacks. To secure the network, apply a distributed or behaviour-based attack detection system and provide a more reliable network.

9	Secure Authentication for Vehicular Ad Hoc Network	Rinsu Aravind, Deepa P L, 2016, International Journal of Computer Science Trends and Technology (I JCS T) [15].	Secure and private vehicular ad hoc networks (VANETs) rely heavily on authentication based on the group signature. Vehicles on vehicular ad hoc networks (VANETs) frequently employ group signatures to bypass authentication. Members of a group can use the group signature method to authenticate communications sent on the group's behalf. A single group public key can be used to verify many signatures without revealing the signer's identity. A vehicle must first validate the sender's group signature to ensure the message is legitimate before proceeding to check the certificate revocation list (CRL) to ensure it is not talking with revoked vehicles. The PKI verifies the identity of each user. Asymmetric key cryptography is the foundation of this system. Our technique maintains conditional privacy in VANETs,	In this paper, they use cryptography techniques to secure VANET, which requires a static network. In the future, we will use distributed, decentralized systems to secure VANET in dynamic environments. Further retrieve the results in terms of percentage of reliability, percentage of attack detection, identification of attack types and impact of QoS on the network.
			although it is more efficient in terms of authentication speed, as shown by our security and performance studies.	
10	Efficient Privacy Preserving Authentication for Vehicular AdHoc Networks	S. Supriya, and B. Bharathi, 2015, Asian Research Publishing Network (ARPN) [16].	This article examines the various authentication protocols currently in use for privacy-preserving authentication in the VANET. Vehicular networks are a rapidly advancing research issue that has applications in fields such as traffic efficiency improvement and safety application. VANET (Vehicular Ad-Hoc Network) is regarded as an intelligent transportation system in which vehicles can connect with one another and with roadside infrastructure. As a result of the ad-hoc nature of the message exchange between two vehicles, the driver's behaviour, and the extreme mobility of the vehicles, privacy and security issues are possible. Authentication is also a concern for any secure interactions because the VANET is insecure and un-trusted.	In this paper, they apply an authentication system for privacy preservation in the VANET network, which requires a static topology. In the future, the system will be enhanced by a collaborative security system that monitors and secures the VANET in a dynamic network.

11	Efficient authentication approach for highly dynamic vehicular ad hoc networks	Kanika Grover, Alvin Lim and Seungbae Lee, 2015, Inderscience Enterprises Ltd. International Journalof Ad Hoc and Ubiquitous Computing [17].	A significant amount of mails expire in the verification queue as a result of this title. Taking into account time-bound VANET broadcast messages verified using complicated ECDSA verification, we present a probabilistic verification for highly mobile and dynamic vehicles to improve packet loss ratio. In addition to our clever authentication technique, we protect the conditional anonymity of automobiles through a streamlined registration procedure.	In this article, they apply the ECDSA verification technique for the authentication of vehicular nodes in VANET. Further improvement is required to improve that process by applying network security techniques in dynamic networks to overcome the data dropping during transmission time.
12	Cognitive radio for vehicular ad hoc networks(CRVANETs): approaches and challenges	Kamal Deep Singh, Priyanka Rawat and Jean-Marie Bonnin, 2014, EURASIP Journal on Wireless Communication s and Networking [18].	This paper examines unique approaches and research issues associated with the application of cognitive radio technology in vehicle ad hoc networks. They discuss how CR technologies such as dynamic spectrum access, adaptive software-defined radios, and cooperative communications will improve vehicular communications and hence have the potential to revolutionize vehicle communication in terms of efficiency and safety. The work differs from previous research in that we present recent advances and open research directions on applying cognitive radio in vehicular ad hoc networks	In this article, they use cognitive radio technology in VANET, which helps to provide cooperative communication and is able to improve the efficiency and safety of VANET. That existing cognitive radio system is further useful for developing the secure

			(CR-VANETs) with an emphasis on architecture, machine learning, cooperation, reprogram ability, spectrum management, and QoE optimization for infotainment applications. Furthermore, offered is a taxonomy of current developments in cognitive radio for vehicle networks. In addition, a number of obstacles and prerequisites have been identified.	VANET and improving network reliability.

13	Privacypreserving Authentication Schemes for vehicular Ad hoc Networks: a survey	Huang Lu, and Jie Li, 2014, Wireless Communication s and Mobile Computing [19].	In this title, they specifically provide a survey on the privacy-preserving authentication (PPA) schemes proposed for VANETs. They investigate and categorize the existing PPA schemes by their key cryptographies for authentication and the mechanisms for privacy preservation. We also provide a comparative study/summary of the advantages and disadvantages of the existing PPA schemes. Lastly, the open issues and future objectives are identified for PPA in VANETs.	In this paper, the author applies the privacy-preserving authentication scheme for VANET security, but it requires a centralized controller. In the future, that work will simulate a dynamic environment to resolve the problem of security from network layer attacks.
14	Privacy Preserving Authentication for Security in VANET	Mahalakshmi.R. S, Alangudi Balaji.N, 2014, IJARCST [20].	n this title they focus of Vehicular Communication, a Vehicular ad-hoc network (VANET) is facing problem with vehicle anonymity and location privacy while communicating among the vehicle. To address this issue, the Vehicular Public Key Infrastructure (VPKI) has been implemented. Given the vital nature of safety applications, VANET security becomes incredibly important. Authentication is a fundamental need for preventing attacks on both intervehicle and vehicle-to-roadside communication in VANET. Vehicles must be protected from the misuse of their private data and privacy breaches. On the assumption that each safety message contains the location information of the sending vehicle, VPKI is an effective technique utilized for security purposes and urban road scenarios. In this title, a distributed Vehicular Public Key Infrastructure is employed to secure VC and protect the privacy and anonymity of vehicle location information. To assure safety The RSA key generating method has been implemented. RSA is a network environment technique that employs public key cryptography.	In this article, they focus on developing security systems using public key cryptography for data security. In the future, secure the vehicular network from the network layer attack, which is useful for reliable communication and improve the performance of the network.

Future Objective of Sybil Attack Detection

Wireless devices in a VANET relay data to neighbouring automobiles, and drivers can communicate with one another through radio waves. Therefore, VANET can improve security and enhance efficiency in transportation. As with every technology, VANET has its fair share of obvious and serious flaws. One of the most crucial is protection against a Sybil attacker, who uses a network to assume several identities across a set of nodes. Since anybody within VANET radio range may connect to the network, it is a prime target for hackers. In this brief, I focus on security concerns, one of the most pressing challenges in vehicle ad hoc networks. The proposed scheme will identify the attacker's symptoms on the basis of:

Participating in routing with unwanted fake identification that consume the limited bandwidth and processing capability of mobile nodes.

Identify malicious nodes that will generate a fake identification and dropped data in network.

When compared to the designed network, the number of packets dropping is higher than expected.

Receiving packets is reduced during an attack, but it improves after security is applied.

Conclusion & Future Work

In this study paper, we get information about the characteristics of VANET, types of attacks, various security schemes for preventing vehicular ad hoc networks, and the objective of detecting Sybil attacker nodes. The literature survey covers various types of attacks, their security systems, and further objectives to improve the system's performance. In this investigation, we focus on getting knowledge about various attacks and security measures and conclude that [7, 8] analyses the effect of a sybil attack and secures VANET using an authentication system [9, 10] detects wormholes and blackhole attacks using a traffic management system; similarly, some of the authors use the concepts of key management authentication systems, MAC layer base security systems, and privacy-preserving authentication systems to provide security to vehicular ad hoc networks.

References

[1] Arun Singh Kaurav and Sushama Rani Dutta, “Detection and Prevention from Different Attacks in VANET: A Survey,” International Conference on Physics and Energy 2021 (ICPAE 2021), pp.1-10, 2021.

[2] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures. Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). National Advanced IPv6 Center, Universiti Sains Malaysia Penang, Malaysia. June 28, 2010.

[3] Divyalakshmi Dinesh, Manjusha Deshmukh, “Challenges in Vehicle Ad Hoc Network (VANET)”IJETMAS, Vol. 2(7), December 2014.

[4] Ghassan Samara, Wafaa A.H. Al-Salihy, R. Sures, "Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)", National Advanced IPv6 Center, University Sains Malaysia Penang, Malaysia. June 28, 2010.

[5] Bassem Mokhtar, Mohamed Azab “Survey on Security Issues in Vehicular Ad Hoc Networks” ELSEVIER Alexandria University Alexandria Engineering Journal Received 28 January 2015; accepted 22 July 2015Available online 18 August 2015.

[6] Muhammad Sameer Sheikh, Jun Liang and Wensong Wang, “A Survey of Security Services, Attacks, and Applications for Vehicular Ad Hoc Networks (VANETs) ,” MDPI Sensors, pp. 1-40, 2019.

[7] Nirbhay Kumar Chaubey, Dhananjay Yadav, “Detection of Sybil attack in vehicular ad hoc networks by analyzing network performance” International Journal of Electrical and Computer Engineering (IJECE), Vol. 12, No. 2, pp. 1703-1710, April 2022.

[8] Mustafa Maad Hamdi, Al-Maarif Sami Abduljabbar Rashid, Majeed Dhafer, Ahmed Jamal Ahmed , Ahmed Shamil Mustafa Ahmed Muhi Shantaf, “Effect Sybil attack on security Authentication Service in VANET,” IEEE International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), June 2022.

[9] Gaurav Soni, Kamlesh Chandravanshi, M.K Jhariya, Arjun Rajput, “An IPS Approach to

Secure V-RSU Communication from Blackhole and Wormhole Attacks in VANET, Contemporary Issues in Communication, Cloud and Big Data Analytics, pp. 57-65, 2022.

[10] Gaurav Soni, Kamlesh Chandravanshi, A Novel Privacy-Preserving and Denser Traffic Management System in 6G-VANET Routing Against Black Hole Attack, Sustainable Communication Networks and Application(ICSCN21), pp.649-663, 2022.

[11] Paramjit Singh Waraich, Neera Batra, "Prevention of Denial-of-Service Attack Over Vehicle Ad hoc Networks using Quick Response Table",IEEE4th International Conference on Signal Processing, Computing and Control (ISPCC), pp.586-591, 2017.

[12] Shamuyarira K and Saraswathi K "The Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Network"International Journal of Recent Scientific Research, Vol. 8 (10), pp. 20557-20560, October, 2017, Received 15th July, 2017Received in revised form 25th August, 2017.

[13] Caixia Song, Guozhen Tan and Chao Yu "An Efficient and QoS Supported Multichannel MAC Protocol for Vehicular Ad Hoc Networks"mdpi Sensors 2017, 17, 2293; doi:10.3390/s17102293.

[14] Kanika Grover, Alvin Lim,"Performance Comparison between Broadcast Authentication Methods for Vehicular Networks" ICINS '16, December 28-31, 2016, Kuala Lumpur, Malaysia© 2016 ACM.

[15] Rinsu Aravind, Deepa P L, "Secure Authentication for Vehicular Ad Hoc Network "International Journal of Computer Science Trends and Technology (I JCS T) – Volume 4 Issue 4, Jul - Aug 2016. 10

[16] S. Supriya, and B. Bharathi, "Efficient Privacy Preserving Authentication for Vehicular Ad-Hoc Networks" Asian Research Publishing Network (ARPN). Vol. 10, No. 20, November, 2015.

[17] Kanika Grover, Alvin Lim and Seungbae Lee "Efficient authentication approach for highly dynamic vehicular ad hoc networks"2015 Inderscience Enterprises Ltd.International Journalof Ad Hoc and Ubiquitous Computing, Vol. 19, Nos. 3/4, 2015.

[18] Kamal Deep Singh, Priyanka Rawat and Jean-Marie Bonnin, "Cognitive radio for vehicular ad hoc networks(CR-VANETs): approaches and challenges" Springer Singh et al. EURASIP Journal on Wireless Communications and Networking 2014, 2014:49.

[19] Huang Lu, and Jie Li, "Privacy-preserving Authentication Schemes for vehicular Ad hoc Networks: a survey" Wireless Communications and Mobile Computing Published online 19 November 2014 in Wiley Online Library.

[20] Mahalakshmi.R.S, Alangudi Balaji.N, "Privacy Preserving Authentication for Security in VANET" (IJARCST 2014) © 2014, IJARCST All Rights Reserved 200 Vol. 2(1) Jan-March 2014.