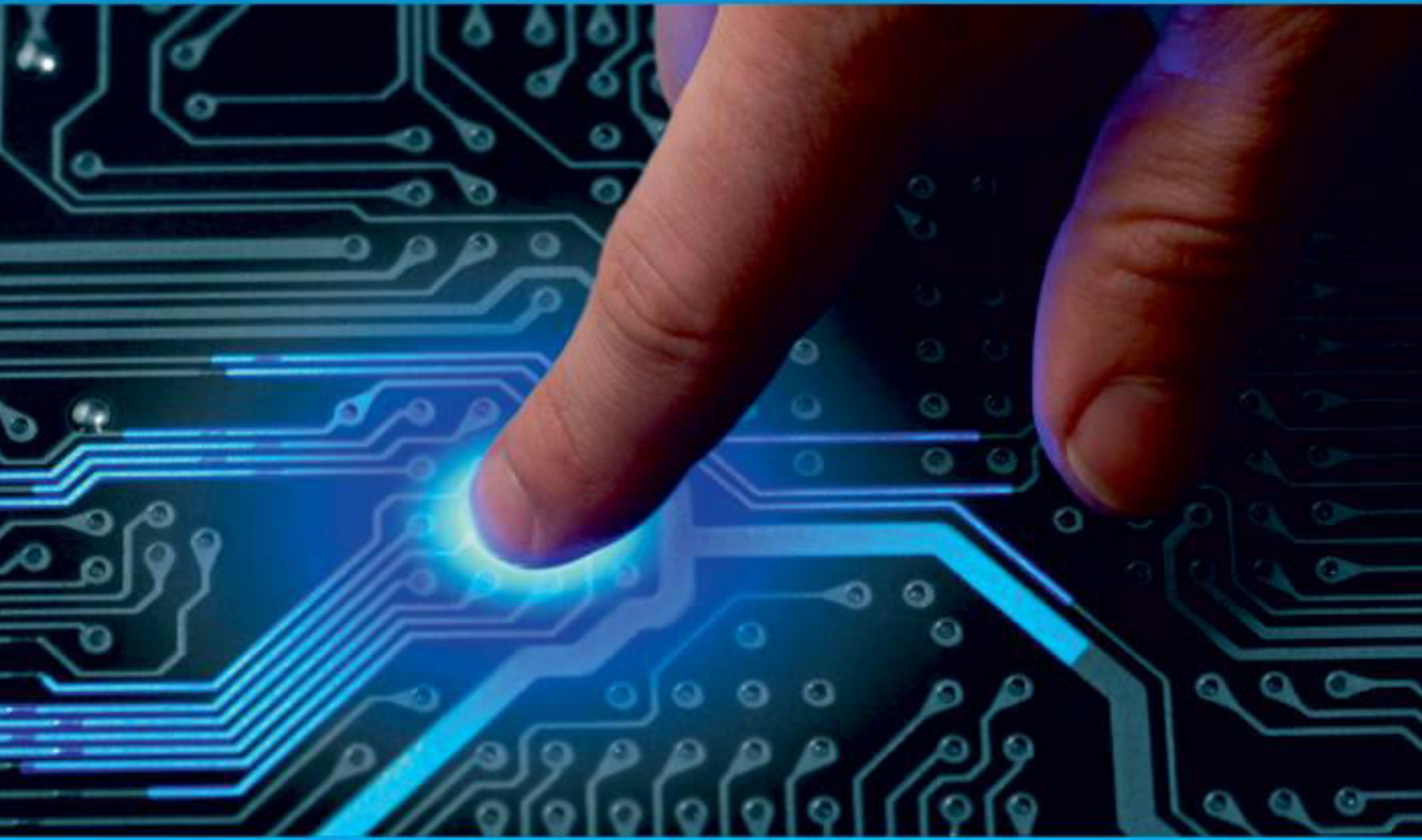
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 2, February 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

| DOI: 10.15680/IJIRCCE.2022.1002024 |

Vehicular Ad-Hoc Networks (VANETs): Architecture, Characteristics, Security Concerns and Overview on Various attacks in VANETs

R. K. Dhuware[1], Tanuj Meshram[2]

Assistant Professor and Head, Department of Computer Science, D.B.Science College, Gondia, India

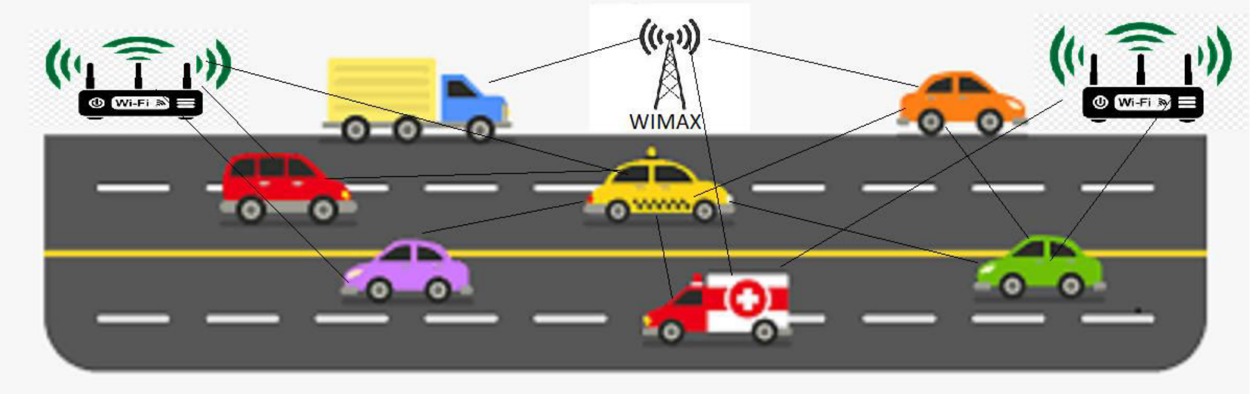
Assistant Professor, Department of Computer Science and Application, Atlanta College, Nagpur, India

ABSTRACT: Wireless technology provides the ability to communicate between two or more entities over a distance without the use of any cable or wire. Wireless communication (or simply wireless) is the transfer of information between two or more nodes that do not use an electrical conductor as a medium by which the transfer is carried out. The most common wireless technologies use radio waves. With radio waves, the intended distance can be short, such as a few meters for Bluetooth or millions of kilometers for deep-space radio communications. The security of nodes is one of the major implications present in VANET. VANET is a subset of MANET and It is increasingly used to avoid accidents, manage traffic control, and also toll stations in public areas. In this paper, we will study different types of VANET attacks, Architecture, Characteristics, and their Security Concern

KEYWORDS: Wireless technology, Deep-space radio communications, Traffic control, VANET attack.

I. INTRODUCTION

The intelligent vehicle is developing technology with a promising future. However, To guarantee the safety of such technology, vehicles must be able to communicate with each other and disseminate information in a real-time environment. VANETs (vehicle ad-hoc networks) were created to meet this need. VANET is classified from MANET (mobile ad-hoc network) with defined established routes. It allows vehicles to transmit information such as location, telemetry data, and safety and security warnings. The prime objective of VANET is to ensure safe driving by improving traffic flow and therefore significantly reducing car accidents. This is possible by providing accurate information to the driver or vehicle.VANETs are a key part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs are referred to as Intelligent Transportation Networks.[1] They are understood as having evolved into a broader "Internet of vehicles".[2] which itself is expected to ultimately become an "Internet of autonomous vehicles".[3]



II. THE VANET ARCHITECTURE

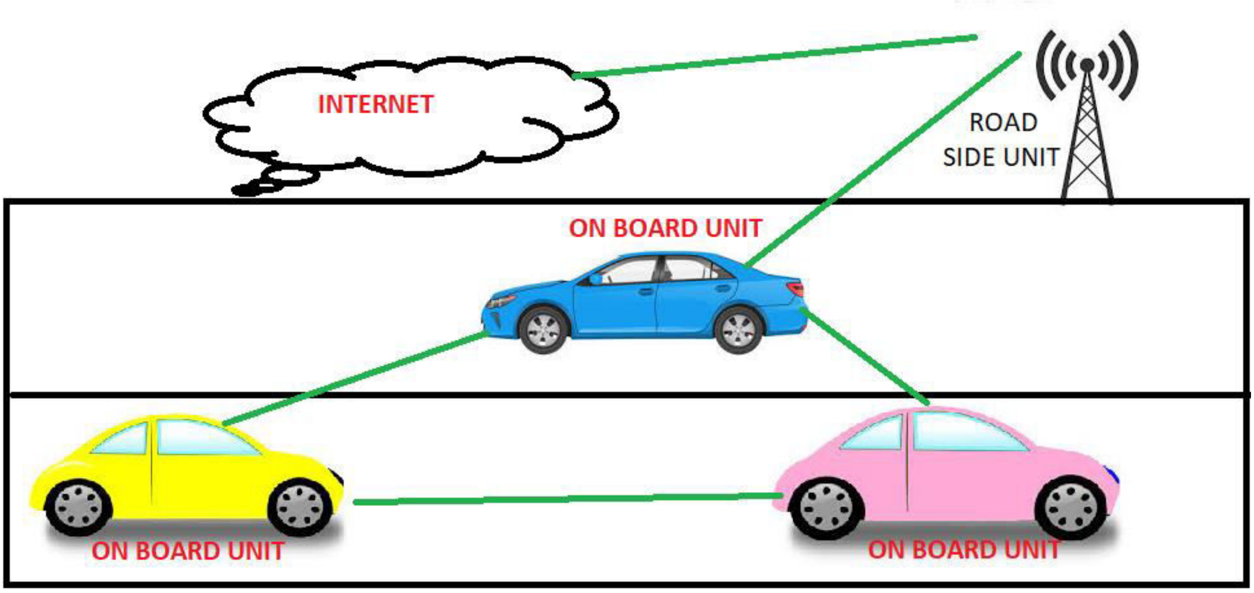
Vehicles participating in a VANET are equipped with a set of wireless sensors and On-Board Units (OBUs). Those units allow wireless communication between the vehicles and their environment. These devices make each vehicle act as a packet sender, receiver, and router. It enables the vehicles to send and receive messages to other vehicles or Road Side Units (RSUs) within their reach via wireless medium [4]. The RSU, normally fixed along the roadside, is equipped with one network device for DSRC (Dedicated Short Range Communication) based on IEEE 802.11p radio technology [5] and can also, be equipped with other network devices to communicate within the network infrastructure

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

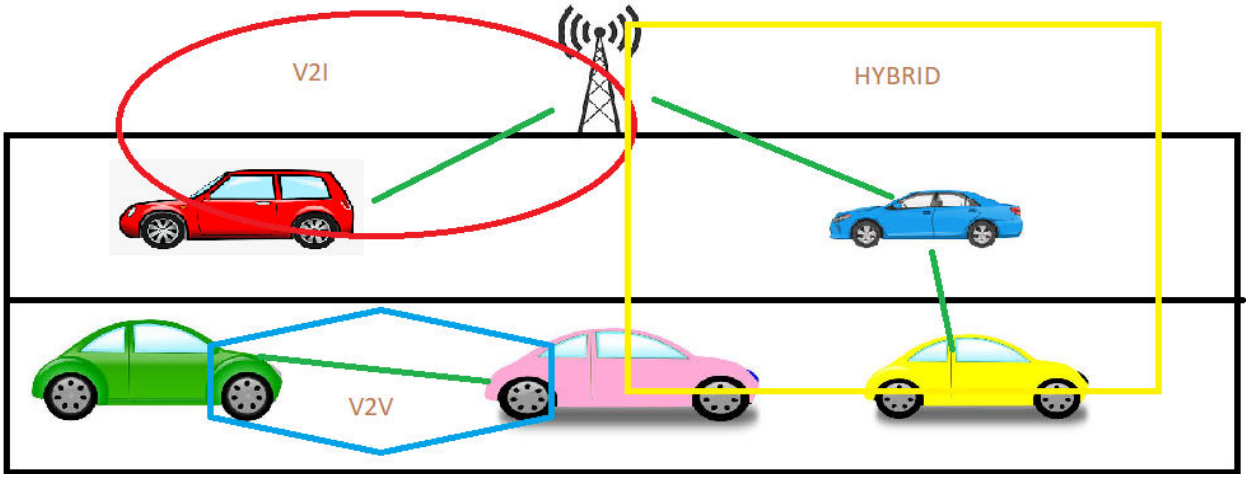
|| Volume 10, Issue 2, February 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1002024 |

[6]. All vehicles move freely on the road network and mainly communicate within each other or with RSUs, as can be seen in Fig. 1 Example of OBU and RSU at work. RSU work as an information source and provides internet connectivity to the OBUs



Vehicles can communicate directly with each other using DSRC in a single or multi-hop way. The communication mode is either V2V (vehicle-to-vehicle), V2I (vehicle-to-infrastructure), or hybrid [7], as can be seen in Fig. 2. These vehicular communication configurations rely heavily on the acquisition of accurate and up-to-date kinematic data from both the vehicles and the surrounding environment with the aid of positioning systems and intelligent wireless communication protocols.



III. VANET CHARACTERISTICS

The collection of interconnected vehicles, VANETs present some distinctive characteristics not seen in other types of MANETs (eg, smartphone/Mobile-based ad-hoc networks).

1) Deploying a VANET is usually expensive because each VANET node (i.e., a vehicle) must contain a rich set of sensors (e.g., LIDAR and proximity sensors) as well as computation and communication resources (e.g., processors, memory, and communication antennas) to analyze and exchange information [6].

2)Moreover, VANETs tend to use short-distance communication (i.e., messages are primarily typically sent when vehicles are close to each other), relegating long-range signals to some special scenarios (e.g., when vehicles need to communicate with roadside units in less populated areas).

3)The life span of a VANET link is short as it is highly affected by the movement of vehicles As a consequence, the network topology tends to change often and thus impose strict latency and bandwidth requirements for applications.[8]
4) VANETs also have predictable mobility patterns as node movements are constrained by the road topology and node locations must be very precise as any vaguely estimated vehicle location can put human lives in danger (e.g., by causing two vehicles to collide).
5) VANETs have no issues concerning power constraints as vehicles can provide a continuous source of power via long-life batteries. [9]
All these features enable VANET to be used in a wide range of dimensions including safer driving improved passenger comfort and increased traffic efficacy.

IV. SECURITY CONCERNS, SECURITY STIPULATION, ATTACKERS, AND ATTACKS IN VANETS

IV(A) Security Concerns: VANETs introduce a new security dimension, which is important for the researcher to deal with In addition, a small number of RSUs, Mobility, not enough wireless connectivity, and basic driver challenges. Imagine a future where vehicles talk to one another and This connected Vehicular technology can change our transportation system as we know it by enabling safe interoperable network wireless communication among vehicle infrastructure and personal communications devices. Intelligent Vehicular system and growing demand for intelligent vehicles on the road, so Safety is becoming a major concern in VANETs because they are directly related to human beings' life

IV (B) Security stipulation in VANETs: For a secure and reliable vehicle network, several security requirements must be considered. Some of these security stipulations for the Vanet is as follows

1. Authentication: Every message in-vehicle communication network must be authenticated, ensure that it originated from authenticating source. Without authentication, illegitimate users and malicious users can insert false messages into the existing network and mislead other vehicles by distributing false information and this could be dangerous.

2. Availability: The vehicular network must be available at all times to their authenticated node, many applications will require in real-time, these applications require a rapid response from sensor networks, seconds for some applications Delay in will make the message meaningless and probably the result will be disastrous anything could happen.

3. Access control: It ensures that only authorized vehicles get quality services on VANET to enhance the driving experience.

4. Confidentiality: The shared public key ensures confidentiality that the designated receiver has access to confidential data, while external nodes may not be able to get access to that confidential data until confidential.

5. Integrity: The exchange of information between the source and the receiver end should be free from change attacks. Thus, the information can be free from alternation and ultimately prevent attackers from modifying any information and making the message content credible.

6. Non Repudiation: Non-repudiation will facilitate the ability to identify attackers even after an attack. This prevents fraudsters from denying their crimes.

7. Privacy: Privacy is one of the most important stipulations in VANET. It must ensure that the identity of the drivers and the location of the vehicles are not disclosed. Anyone does not like to disclose private information and this must be the prime concern.

IV(C).Attackers in VANETs:

To secure VANET, first, we need to find out who the attackers are, their nature, and their potential to cause harm System. Attackers can be of any category based on the following types it may be

Insider: This type of attacker is an authentic user of the network and has detailed knowledge of the network. If the attacker may be a member node who can communicate with other members of the network, it'll be referred to as an Insider and ready to attack in various ways.

Outsider: The outsider attacker is a kind of intruder who aims to misuse the protocols of the network and the range of such attacks are limited which means less variety of attacks, maybe Active and Passive

Active and Passive attackers: Active attackers generate signals or packets whereas passive attackers only sense the network

Other attackers: other attackers may be in the following category:[10,11] Vandal: This kind of attacker is ill-motivated. They just want to show their abilities to attacks. Hacker: The hacker is motivated by enthusiasm and interest without getting back any benefit from the attack. Malicious hacker: The malicious hacker is driven by the monetary purposes of the organization or for personal/political gain.[10]

IV(D)Attacks in VANETs:

1. Denial of Service (DoS) Attack: In Denial of Service (DoS) attack, the attacker takes control of the vehicular resources to transmit dummy messages or disseminate forged messages which make the network unusable to the legitimate vehicles. It means that the attacker jams the vehicle's communication channel by creating so many messages under attack that legitimate messages are not transmitted. The attack causes VANET to lose its ability to provide services to legitimate vehicles resulting in decreased network performance.[12].

2. Black Hole Attack: In Black Hole attack, the attacking node pretends to have the shortest path to the destination and fascinates the source node to route through this node by providing the fake routing information. This way the source node transmits the data through a malicious node considering the path as the shortest route between the source and destination. This attack results in dropping or misusing the intercepted packets by malicious nodes without forwarding them.[12]

3. Wormhole Attack: In Wormhole attack, a tunnel is created by two or more malicious nodes in the network. The packets received by any malicious node at one end of the tunnel in the network are tunneled to another malicious node at other ends of the tunnel and then these packets are retransmitted into the network. This attack prevents the discovery of valid routes in the network.[12]

4. Grayhole Attack: The grayhole attack resembles the black hole attack in a manner that it doesn't absorb or drop all the incoming packets as in the blackhole attack but it drops selective packets and forwards the rest of the packets to the destination node. Grayhole attack is hard to detect because initially, the attacking node behaves as an honest node during the route discovery process, but then silently drops some of the data packets not only due to its malicious nature but also sometimes due to selfish nature, congestion or overload.[12]

5. Illusion Attack: In illusion attacks, the adversary deceives purposefully the sensors on his car to produce wrong sensor readings and thus incorrect traffic information. As a result of this, the corresponding system reaction is invoked and then it broadcast the incorrect traffic warning messages to neighbors. Thus, an illusion Attack is successfully launched by the Attacker.[12]

6. Sybil Attack: In Sybil attack, the attacking node sends messages with multiple identities to other nodes in the network and creates an illusion of the existence of multiple vehicles in the network. In this way, the attacker takes the control of the complete vehicular network to inject fake messages into the network. This attack impairs the functionality of the whole network.[12]

7. Sinkhole Attack: In Sinkhole attack, all the network traffic is attracted by the attacker by broadcasting the fake routing information. This attack results in degradation of the network performance either by dropping the data packets or by modifying them.[12]

8. Timing Attack: The main objective of the attacker is to add some time slot in the original message that creates a delay in the original message and these messages are received after these required times. AS we know safety applications are time-critical applications if a delay occurs in these applications then the major objective of these applications is also finished.[13]

9. Node Impersonation Attack: In a vehicular network, each vehicle has a unique identifier that is used to verify the messages whenever the accident occurs by sending the wrong messages to other vehicles[14]

10. Application Attack: The main motive of the attacker in this kind of attack is content that is related to safety and non-safety-related applications. Safety applications play a very important role as they provide warning messages to other users. In this attack, the attackers alter the contents of the actual message and send wrong messages to other users."[15],[16]"

11 Non-Safety Application Attack: Non-safety is related to users' comfort during the journey. These do not disturb the safety applications. The main role of non-safety applications is to give comfort to passengers and to improve the traffic system. One of the major non-safety applications is car parking.[17],[18]

V. RELATED WORK

In 2011 Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan published a paper on, "Vehicular ad hoc networks (VANETS): status results and challenges". They outline some of the VANET research challenges that still need to be addressed to enable the ubiquitous deployment and widespread adoption of scalable, reliable, robust, and secure VANET architectures, protocols, technologies, and services.[16]

In 2014 Mario Gerla, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee published a paper on Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds. In this article, they discuss the evolution from Intelligent Vehicle Grid to Autonomous, Internet-connected Vehicles, and Vehicular Cloud.[3]

In 2014 Elias C. Eze, Sijing Zhang, Enjie Liu, Joy C. Eze published a paper on Advances in Vehicular Ad-Hoc Networks (VANETs): Challenges and Road-map for Future Development. This paper provides an overview on current research state, challenges, potentials of VANETs as well the ways forward to achieving the long-awaited ITS.[4]

In 2015 Indu Bhardwaj and Sibaram Khara published an Article: An Analytic Study of Security Solutions for VANET. International Journal of Computer Applications. This paper presents a review of security requirements, attacks and security challenges to implement the security measures in the VANET. Existing solutions proposed by different researchers are also reviewed and compared to find out the research gaps and scopes in the field of VANET security.[12]

In 2015 Ujwal Parmar, Sharanjit Singh published a paper on "Overview of Various Attacks in VANET" In this paper, they present a comprehensive study of various attacks in VANET and a comparison of various attacks in VANET.[13]

In 2017 Fatih Saki and Sevil Sen published a paper on A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV. This paper aims to survey possible attacks and the corresponding detection mechanisms that are proposed in the literature. The attacks are classified and explained along with their effects, and the solutions are presented together with their advantages and disadvantages. An evaluation and summary table which provides a holistic view of the solutions surveyed is also presented.[2]

In 2017 Hasrouny H, Samhat AE, Bassil C, Laouiti A published a paper on VANet security challenges and solutions: A survey. In this paper, they give the details of the recent security architectures and the well-known security standards protocols. The second focuses on a novel classification of the different attacks known in the VANET literature and their related solutions. The third is a comparison between some of these solutions based on well-known security criteria in VANET. Then they draw attention to different open issues and technical challenges related to VANET security, which can help researchers for future use.[7]

VI. CONCLUSION

Security is the major issue in implementing the VANET. In this paper, the security stipulation, security attacks, attackers, Architecture, Characteristics, and Security Concerns of VANETs are discussed. Also, the various related work by different researchers is briefly discussed. We study a different facet of VANET. We can conclude that there is still a need for extensive research in the area of security issues and solutions. This paper will be beneficial for the students and researchers in the domain of VANETs

REFERENCES

1. Research Challenges in Intelligent Transportation Networks, IFIP Keynote, 2008
2. Sakiz, Fatih; Sen, Sevil (June 2017). "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV". Ad Hoc Networks. 61: 33–50. doi:10.1016/j.adhoc.2017.03.006.
3. Gerla, M.; Lee, E.; Pau, G.; Lee, U. (March 2014). "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds". 2014 IEEE World Forum on Internet of Things (WF-IoT): 241–246. doi:10.1109/WF-IoT.2014.6803166. ISBN 978-1-4799-3459-1. S2CID 206866025.
4. Eze EC, Zhang S, Liu E (2014) Vehicular ad hoc networks (VANETs): Current state, challenges, potentials and way forward in 2014 20th International Conference on Automation and Computing, 176–181.. IEEE.
5. Jiang D, Delgrossi L (2008) IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments in VTC Spring 2008-IEEE Vehicular Technology Conference, 2036–2040.. IEEE.
6. Al-Sultan S, Al-Doori MM, Al-Bayatti AH, Zedan H (2014) A comprehensive survey on vehicular ad hoc network. J Netw Comput Appl 37:380–392.
7. Hasrouny H, Samhat AE, Bassil C, Laouiti A (2017) Vanet security challenges and solutions: a survey. Veh Commun 7:7–20.
8. Lee KC, Lee U, Gerla M (2010) Survey of routing protocols in vehicular ad hoc networks in: Advances in Vehicular Ad-hoc Networks: Developments and Challenges, 149–170. IGI Global.
9. Jakubiak J, Koucheryavy Y (2008) State of the art and research challenges for VANETs in: 2008 5th IEEE Consumer Communications and Networking Conference, .912–916. IEEE.
10. Mohammed Ali Hezam Al Junaid; Syed, A A; Mohd Nazri Mohd Warip; Ku Nurul Fazira Ku Azir; Romli, Nurul Hidayah. MATEC Web of Conferences; Les Ulis, Vol. 150, (2018). DOI:10.1051/matecconf/201815006038
11. C. Y. Shim, "A taxonomy for DOS attacks in VANET," 2014 14th Int. Symp. Commun. Inf. Technol., pp. 26–27, 2014
12. Indu Bhardwaj and Sibaram Khara. Article: An Analytic Study of Security Solutions for VANET. *International Journal of Computer Applications* 132(10):1-7, December 2015. Published by Foundation of Computer Science (FCS), NY, USA.
13. Ujwal Parmar, Sharanjit Singh- Astt.Prof. M.tech (CSE) Student - M.tech (CSE) Guru Nanak Dev University RC Gurdaspur, India-2015 on "Overview of Various Attacks in VANET"
14. T.Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Improved security in Geographic ad hoc routing through

autonomous Position Verification", ULM University

15. Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in VANET," IJNSA, Vol.3, No.6, November 2011.
16. Sherali Zeadally, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, Aamir Hassan, "Vehicular ad hoc networks (VANETS): status results and challenges", springer science+ Business Media, LLC 2011.
17. T.Leinmuller, E. Schoch, F. Kargl, C. Maihofer, "Improved security in Geographic ad hoc routing through autonomous Position Verification", ULM University.
18. M. Raya, P. Papadimitratos, J.P. Hubaux," Secure vehicular communications", IEEE Wireless Communication Magazine, special issue on inter-vehicular communication, Oct 2006.

BIOGRAPHY

R. K. Dhuware is an Assistant Professor and Head in the Department of Computer Science, D.B.Science.College, Gondia RTM Nagpur University, India. He received Ph.D. in 2019 from RTM Nagpur University, India. His area of Specialization is Computer Networks, Data Mining, Elearning, Network Security management**.**

Tanuj Meshram is an Assistant Professor in the Department of Computer Science and Application, Atlanta College, Nagpur RTM Nagpur University, India. He received Master of Computer Application (MCA) degree in 2015 from RTM Nagpur University, India. His research interests are Computer Networks, Algorithms, Programming.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

📱 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com