

Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey

Amit Kumar Goyal

Department of Computer Applications, KIET Group of Institutions, Ghaziabad, 201206, India
E-mail: athroam@gmail.com

Gaurav Agarwal

Department of Computer Science and Engineering, Invertis University, Bareilly, 243123, India
E-mail: gaurav.a1@invertis.org

Arun Kumar Tripathi

Department of Computer Applications, KIET Group of Institutions, Ghaziabad, 201206, India
E-mail: mailtoaruntripathi@gmail.com

Received: 22 July 2019; Accepted: 23 August 2019; Published: 08 October 2019

Abstract—The density of traffic is increasing on the daily basis in the world. As a result, congestion, accidents and pollution are also increasing. Vehicular Ad-hoc Network (VANET), a sub class of Mobile Ad-Hoc Network (MANET), is introduced as solutions to manage congestion and accidents on roads. VANET is gaining attention among researchers due to its wide-range applications in the field of Intelligent Transportation System (ITS). The paper focus on communication architectures along with its components and access technologies, challenges and security attacks in VANET. Furthermore, it deals with broad categorization various research domains, research methodologies and research models in VANET. At last, paper explores various application area of VANET.

Index Terms—VANET, Architecture, Security, Challenges, Attacks, Research Models.

I. INTRODUCTION

According to the survey in 2018, by World Health Organization (WHO), worldwide more than 1.35 million people are losing their lives every year in roadside accident, which is approximately 3% of that country Gross Domestic Product (GDP) [1]. According to a prediction, road traffic injuries will rise to the fifth cause of death by 2030 as compared to the ninth cause of death in 2004.

Due to increase in per capita income, at present scenario, people are more dependent on private vehicles or paid taxi services. As a result, a number of vehicles increasing on per day basis. Due to unawareness of traffic-rules and massive traffic, accidents on the roads are also increasing in the proportional of traffic. The

safety and shielding of human life on roads is the most challenging issue

VANET [2] is a subclass of Mobile Ad-hoc Network (MANET) having pre-defined routes (roads). The basic objective of VANET is to provide congestion free safer and comfortable journey [2] to passengers.

In VANET, moving vehicles are equipped with specialized sensors, known as On-Board Unit (OBU) [3], which collects information in real time fashion from surrounding moving vehicles or stationery Road Side Units (RSU) [3] and shares it with other moving vehicles directly or with the help of RSUs. It helps in predicting jams and allow nodes to decide a best alternate path [4,5] among the existing once. In reference to VANET, the moving vehicle are known as nodes. For exchange of information among vehicles, there must be a specific and dedicate range of radio frequency spectrum.

The rest of the paper is structured as follows, section II deals with generalized VANET architecture and its components, and Section III discusses insight of various challenges in VANET. Section IV, explores various research domains in VANET, Section V focuses on research domains and methodologies and models for VANET, whereas section VI provides various application areas of VANET and at last, section VII summarizes the work with future trends in VANET.

II. VANET ARCHITECTURE

VANET uses Wireless Access in Vehicular Environment (WAVE) to exchange information between OBUs equipped within vehicles, RSUs and a set of sensor nodes. Fig. 1 shows generalized VANET architecture [6]. The basic units involved in communication are AU, OBU and RSU. These are discussing as follows:

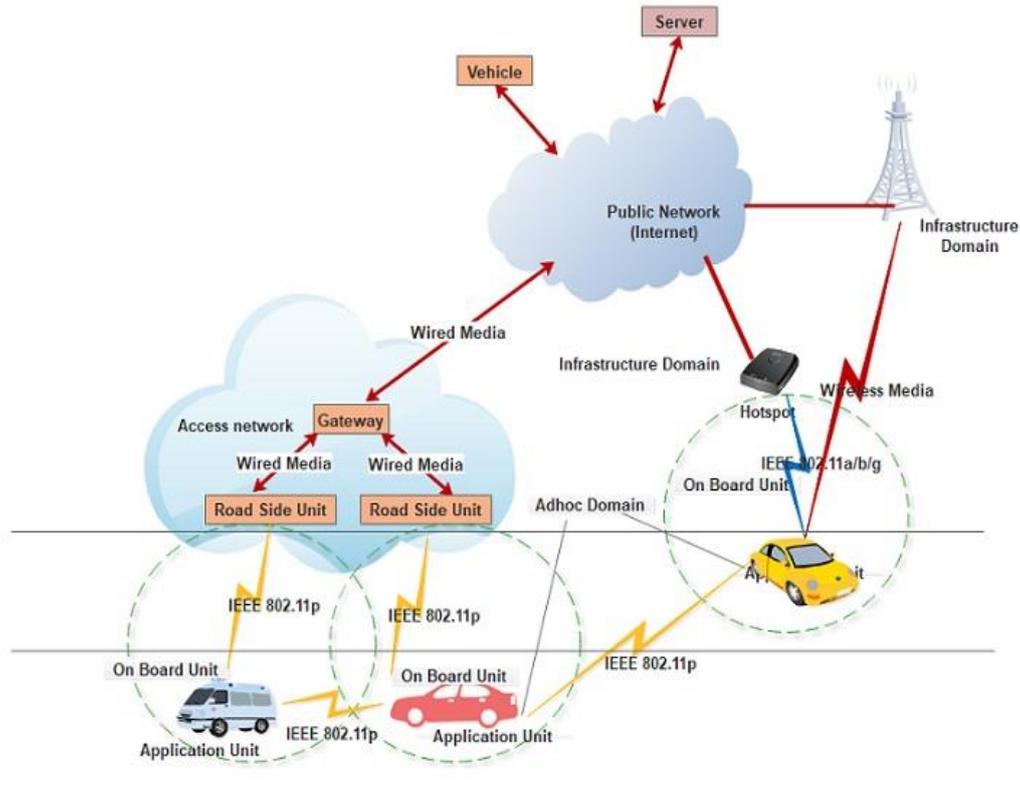


Fig.1. Generalized VANET Architecture

A. Application Unit (AU)

It is a Graphical Interface (GI) between user and OBU. The user can retrieve the stored messages, complete information about journey speed, traffic condition etc. for analysis.

B. On Board Unit (OBU)

It is an electronic device consisting of processor, Global Positioning System (GPS), read/write memory, sensor nodes, and Event Data Recorder (EDR) modules. Sometimes these modules may be placed independently inside the vehicles. Generally, OBUs are mounted on-board and exchange information with nearby OBUs and RSUs. For communication, OBU uses IEEE 802.11p radio technology in ad hoc environment. On the other hand, in infrastructure-based environment, OBUs use IEEE802.11 a/b/g radio technology. Furthermore, OBUs control ad-hoc connection, routing, IP-based mobility management, data security issues and network congestion. EDR is an electronic device and part of OBU. It stores all the transmitted and received messages to the nearby OBUs and RSUs. It also records all activities that happened in vehicle environment during the trip. GPS module is used to identify the physical location acceleration and direction of movement of vehicle at specific interval of time. A special purpose-computing device is attached with OBU. It is responsible for taking necessary action corresponding to messages received from other OBUs or RSUs. Radars and sensors are used to detect obstacles that appear during movement of vehicle. An omnidirectional antenna is responsible for accessing

the information on wireless channels. To identify a vehicle uniquely an Electronic License Plate (ELP) is also associated with every vehicle.

C. Road Side Unit (RSU)

RSUs are stationary units mounted along the roadside. RSUs exchange information through wired or wireless communication mediums. For exchanging information, VANET uses Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) modes. In V2V, vehicles may exchange information directly to other nearby vehicles using single hop technique or using multi-hop technique with the help of intermediate vehicles. In general, safety-related messages are transmitted in single-hop fashion, on the other hand, non-safety-related messages are transmitted in multi-hop fashion.

For this, communication media must have low latency and high transmission rate. In general, V2V mode is used for broadcasting for emergency messages such as emergency braking, collision deceleration, bottleneck alert, etc. Sometimes, V2V communication is also used in cooperative driving. On the other hand, V2I vehicles exchange information with fixed RSUs using GSM, UMTS or WiMAX networks.

III. CHALLENGES IN VANET

In the last decade, there has been a remarkable progress in the field of VANETs. Regardless of advantages, VANETs still suffer from many challenging issues [7,8,9,10]. These are discussed as follows:

A. High Latency

The message transmitted by the OBU should reach to one or more OBUs within the acceptable time duration in VANET. So that, the driver of receiving OBU may have sufficient time to take necessary action corresponding to received message. Since, VANET does not have any central coordinator for bandwidth management and may results, congestion due to limited bandwidth (10-20 MHz) particularly in high-density area. The fair bandwidth management reduces delay for disseminating messages

B. Heterogeneous Networks

The network is one of the critical issues, as different countries have different security and privacy policies and differing available infrastructure and implementation by manufacturers. The protocols used by different networks may be different and this may lead to high latency.

C. High Mobility

VANET has highly mobile nodes. The vehicles move on predefined particular path. Due to high speed the topology changes very rapidly and a node makes connections to RSUs or nearby OBUs of a very short interval. The high mobility rate may cause break-up of ongoing existing connection and establishment of new connection. Frequently disconnection and establishment may cause higher latency. This affects the quality of communication. In addition, it is very difficult to authenticate high-speed moving vehicle. For this, many researchers suggest IPv6 enabled low overhead authentication schemes

D. Privacy

VANET has an association between user and vehicle. Privacy concerns should not disclose the driver's location. Furthermore, the journey may involve the financial truncation. VANET should take care of privacy of transitions involved during the journey.

E. Need of high computational ability

In VANET, vehicles are equipped with large number of sensors and computational resources. The computational ability of these resources, such as GPS, processors, etc., is most challenging issue. Real time computational power helps to obtain current position, speed and direction of vehicle at any moment of time.

F. Irregular Network Density

The network density in VANET is not same under each

RSU. It depends of many factors such as traffic jam, narrow bridges, rural or urban area. In daytime, the traffic may have higher density in comparison to night. Similarly, urban area, highways etc. may have higher density with respect to rural area.

G. Signaling Fading

The obstacles between two communicating vehicles may lead to fading of signals and results decrease in efficiency of VANET. The obstacles may be buildings or any other vehicle.

H. Routing Protocol

To manage high-speed moving vehicles, VANET should have an efficient routing protocol that can deliver the messages within the specified time interval to the destination. Efficient routing may increase the reliability, scalability and decrees in latency in message delivery.

I. Security

Security is the most critical issue of VANET. The security services may lead to secure processing and exchange of messages. The security services include authentication, availability, confidentiality, integrity, non-repudiation, Privacy and anonymity, Data verification, access control, Traceability and revocability, error detection, Liability identification, Vehicle ID Traceability etc.

IV. SECURITY ATTACKS IN VANET

VANET architecture is susceptible to various attacks [11-22] such as unauthorized access; bogus message exchange creating traffic jam, leaking of private information illegal use, eavesdropping, and protocol tunneling, etc. To provide better protection against the attackers, we must have the entire information about the attacks in VANET. The entities that can directly affects the VANET security are RSUs, OBUs, attackers, drivers and third party such as certification authorities. Fig. 2 shows various attacks on different security requirement.

The security mechanisms used in VANET include PKI (Public Key Infrastructure) [23,24,25], TESLA (Timed Efficient Stream Loss-Tolerant Authentication) [26], TESLA++ (Modified version of TESLA) [27], ECDSA (Elliptic Curve Digital Signature Algorithm) [28,29,30,31] VAST (VANET Authentication using Signatures and TESLA++) [32] etc. Most of the researchers are taken above security mechanisms in consideration.

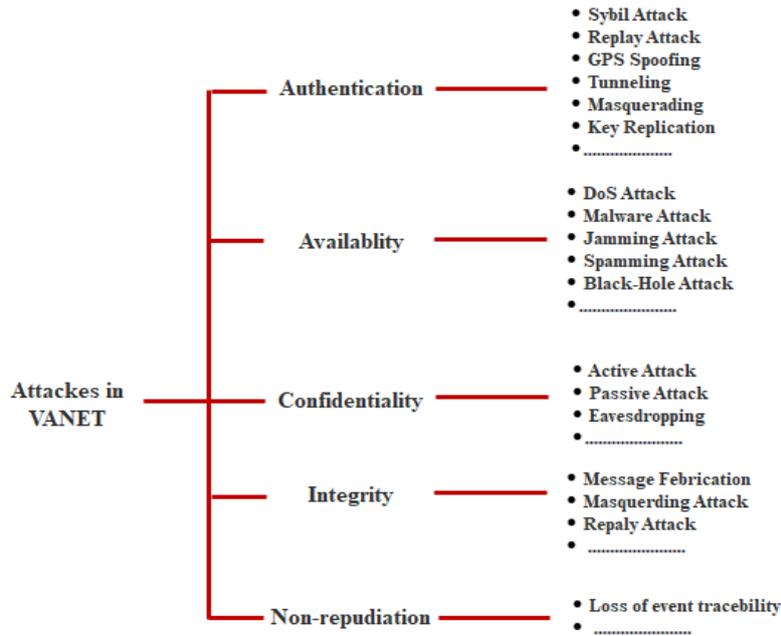


Fig.2. Various attacks on different security requirement

V. RESEARCH DOMAINS IN VANET

In recent years, the different domains [33,34] of VANET have attracted the research community a lot. These domains fall in field of the application layer, MAC

layer, physical layer, performance of network, routing protocol etc. Table 1 gives an overview of various domains in which the research is going on in VANET. Table 1 shows the research domain in the VANET.

Table 1. Research Domain and their description

Domain	Description
Application layer service domain	Focuses on Safety on roads, Efficiency and effectiveness in traffic management, Entertainment for the driver, impact of VANET on Environmental condition
Security related services	Security related issues and their mechanisms, other Quality of services (QoS) such as Location Tracking, Location Estimate and its Correction, Integration with existing Infrastructure
Routing protocol domain	Proposal of a new routing protocol, Protocol design, its testing, and verification analysis is the key for research.
Data collection and Communication domain	techniques for data collection and the information dissemination methods
MAC and Physical layers domain	Techniques / protocols based on MAC, Channel modelling, modulating and coding techniques, Adaptive transmit power control
Mobility domain	Mobility / Connectivity analysis, modelling, management, Clustering Algorithm
Tools, test beds domain	Experimental and Prototype Results are obtained, analysis of proposed architectures after deployment and field-testing is performed.
Performance evaluation domain	This domain having emphasis on Protocol performance analysis and their comparison and applying simulation in order to get the actual result.

VI. RESEARCH METHODOLOGY AND RESEARCH MODELS IN VANET

To evaluate and analyze the performance of a newly proposed algorithm or architecture in VANET an effective research methodology [35] is needed. It helps to compare the newly proposed scheme with existing ones. There are three methodologies to evaluate the

performance of newly suggested scheme named as simulation technique, mathematical model and real-life implementation. Table 2 shows various research methodologies and their description.

VANETs have complex system architecture and system model. These are categorized into four sub models [35]. Table III describes these models in brief.

Table 2. Research Methodologies in VANET their description

Research Methodology	Description
Simulation Technique	It provides a simulated environment as in real-life. It is one of cheap and best method to evaluate the performance of proposed scheme or system with existing one. For VANET Simulation of Urban Mobility (SUMO), OMNET++, OPNET, MATLAB, QualNet simulators are available in the market.
Mathematical Analysis	Now a day most of researchers focusing on mathematical modelling. It provides estimated values as in simulation environment or real-life implementation. It is very cost effective.
Real-Life Implementation	It is best methodology to evaluate the performance of model. It may not feasible due time constraints and higher cost of implementation.

Table 3. Research Models and their description

Model	Description
Driver and Vehicle Model	This model deals with behaviour of driver of a particular vehicle. It mainly focuses on driving styles of driver e.g. violent or inactive and the potential vehicle characteristics such as passenger car or a sports car.
Traffic Flow Model	This model deals with communications between vehicles, drivers, and infrastructures for developing an optimal road-network. The traffic follow model is categorized as microscopic, mesoscopic, and macroscopic.
Communication Model	This model deals with information exchange between two or more vehicles. This model emphasis on evaluation of performance between communicating layers and different routing approaches.
Application Model	This model deals with conduct and quality of cooperative applications.

VII. APPLICATION AREAS OF VANET

The VANET is broadly categorized into two application area named as safety applications and non-

safety/ convenience applications [36]. Fig. 3 shows safety application areas and their specific utilization and Fig. 4 shows convenience application areas and their specific utilization.

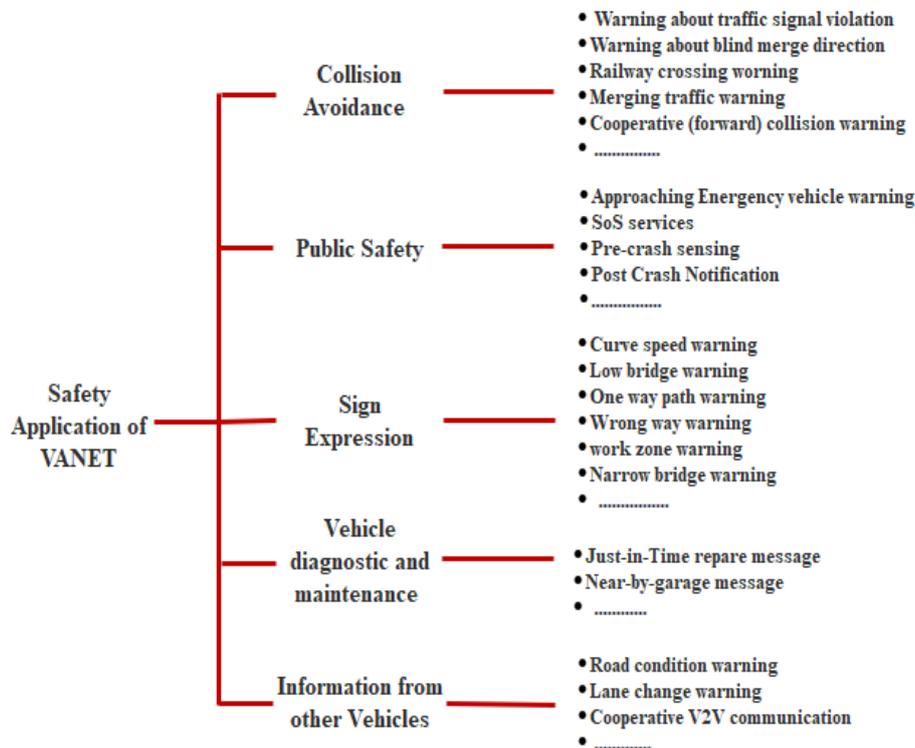


Fig.3. Safety application areas

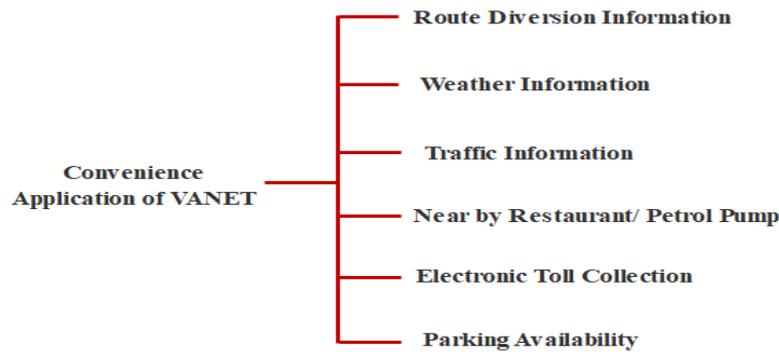


Fig.4. convenience application area

VIII. CONCLUSION

VANET is one of emerging field of MANET. ITS is one of the most demanding application of VANET and taken into consideration for implementation of ITS. VANET focuses on safer, convenient, and pleasant by reducing traveling time, road congestion etc. The paper focuses on safety applications that require VANET for maintaining the comfort and safety for drivers and passengers on the road. The main focus of paper is to describe VANETs communication architectures, its various components, access technologies, challenges and security attacks in VANET. Furthermore, paper introduces various research domains, research methodologies and security issues in VANET. The basic objective of paper is to introduce the VANET with respect to research point of view and motivate to researchers to explore areas in Intelligent Transportation System in smart cities.

REFERENCES

- [1] <https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries>
- [2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular Ad Hoc network", *Journal of Network and Computer Applications*, volume 37, Issue 1, January 2014, pp. 380–392, doi:10.1016/j.jnca.2013.02.036
- [3] Ikram Ali, Alzubair Hassan, and Fagen Li, "Authentication and privacy schemes for vehicular ad hoc networks (VANETS): A survey", *Vehicular Communications* Volume 16, April 2019, pp. 45–61, doi: 10.1016/j.vehcom.2019.02.002
- [4] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: a survey", *IEEE Vehicular Technology Magazine*, Volume 2, Issue 2, June 2007, pp. 12 – 22, doi: 10.1109/MVT.2007.912927
- [5] X. Su, "A comparative survey of routing protocol for vehicular sensor networks", *IEEE International Conference on Wireless Communications, Networking and Information Security*, June 2010, doi: 10.1109/WCINS.2010.5542309
- [6] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks," *IEEE Communications Magazine*, Volume 46, Issue 6, June 2008, pp. 164–171, doi: 10.1109/MCOM.2008.4539481
- [7] M.N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions", Elsevier, *Vehicular Communication.*, Volume 1, Issue 2, April 2014, pp. 53–66, doi:10.1016/j.vehcom.2014.05.001.
- [8] G. Karagiannis, O. Altintas, E. Ekici et al., "Vehicular net-working: a survey and tutorial on requirements, architectures, challenges, standards and solutions" ,*IEEE Communications Surveys and Tutorials*, Volume 13, Issue 4, July 2011 pp. 584–616, doi: 10.1109/SURV.2011.061411.00019
- [9] S. Zeadally, R. Hunt, Y.S. Chen, A. Irwin, A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges", *Springer Telecommunication Systems*, Volume 50, Issue 4, August 2012, pp. 217–241, doi: /10.1007/s11235-010-9400-5
- [10] Arun Kumar Tripathi, R. Radhakrishnan and J. S. Lather, "Impact of wireless link delay on handover latency in Mobile IPv6 environment", *International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT-14)* February 2014, pp. 424–428, 10.1109/ICICT.2014.6781319.
- [11] S.S. Tangade, and S.S. Manvi, "A survey on attacks, security and trust management solutions in VANETS", *Proc. 4th IEEE International Conference on Computing, Communications and Networking Technologies, ICCCNT-2013* , pp. 1–6, doi: 10.1109/ICCCNT.2013.6726668
- [12] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc net-works," *Journal of Computer Security*, Volume 15 Issue 1, January 2007, pp. 39–68, doi: 10.3233/JCS-2007-15103
- [13] Lianhai Liu, Yujue Wang, Jingwei Zhang, and Qing Yang, "A Secure and Efficient Group Key Agreement Scheme for VANET", *MDPI Sensors*, Volume 19 Issue 3, January 2019, pp: 1–14, doi: 10.3390/s19030482
- [14] J. Jeneffa, and E. A. Mary Anita, "Secure Vehicular Communication Using ID Based Signature Scheme", *ACM, Wireless Personal Communications: An International Journal*, January 2018, Volume 98, Issue 1, pp 1383–1411, doi:10.1007/s11277-017-4923-7.
- [15] Sarah Oubabas, Rachida Aoudjit, Joel J. P. C. Rodrigues, and Said Talbi, "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme", Elsevier , Volume 13, July 2018, pp. 128–138, doi:10.1016/j.vehcom.2018.08.001
- [16] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication", *Springer-Verlag Wien* 2016, Volume 98, Issue 7, July 2016, pp: 685–708,

- doi:10.1007/s00607-014-0393-x
- [17] Shihan Bao, Waleed Hathal, Haitham Cruickshank, Zhili Sun, Phillip Asuquo, and Ao Lei, "A lightweight authentication and privacy-preserving scheme for VANETs using TESLA and Bloom Filters", *ScienceDirect ICT Express*, Volume 4, Issue 4, December 2018, pp: 221–227, doi:10.1016/j.ict.2017.12.001
- [18] Jie Li, Huang Lu, and Mohsen Guizani, "ACPN: a novel authentication framework with conditional privacy preservation and non-repudiation for VANETs", *IEEE Transactions on Parallel and Distributed Systems*, Volume 26, Issue 4, April 2015, pp. 938-948, doi: 10.1109/TPDS.2014.2308215
- [19] Cui Li and Ze Wang, "Location-based Security Authentication Mechanism for Ad hoc Network", *Proceeding of National Conference on Information Technology and Computer Science*, November 2012, doi:10.2991/citcs.2012.150
- [20] Mina Rahbari and Mohammad Ali Jabreil Jamali, "Efficient detection of Sybil attack based on cryptography in VANET", *International Journal of Network Security & Its Applications*, Volume 3, Issue 6, November 2011, pp 185- 194, doi: 10.5121/ijnsa.2011.3614
- [21] Xiaodong Lin, Xiaoting Sun, Xiaoyu Wang, Chenxi Zhang, Pin-Han Ho, and Xuemin (Sherman) Shen, "Timed Efficient and Secure Vehicular Communications with Privacy Preserving", *IEEE transactions on wireless communications*, Volume 7, Issue. 12, December 2008, pp: 4987-4998, doi:10.1109/T-WC.2008.070773
- [22] Chenxi Zhang, Xiaodong Lin, Rongxing Lu, Pin-Han Ho, and Xuemin (Sherman) Shen, "An Efficient Message Authentication Scheme for Vehicular Communications", *IEEE transactions on vehicular technology*, Volume 57, Issue 6, November 2008, pp. 3357 - 3368, doi:10.1109/TVT.2008.928581.
- [23] M. Raya, J. Hubaux, "The security of vehicular ad hoc networks", *Proc. 3rd ACM Workshop on Security of Ad hoc and Sensor Networks*, November 2005, pp. 11–21, doi:10.1145/1102219.1102223
- [24] G. Calandriello, P. Papadimitratos, J.P. Hubaux, A. Lioy, "Efficient and robust pseudonymous authentication in VANET", in: *Proc. 4th ACM International Workshop on Vehicular Ad Hoc Networks*, September 2007, pp .19–28, doi:10.1145/1287748.1287752
- [25] A. Wasef, X. Shen, "EMAP: expedite message authentication protocol for vehicular ad hoc networks", *IEEE Transactions on Mobile Computing*. Volume 12 Issue 1, January 2013, pp. 78–89, doi:10.1109/TMC.2011.246
- [26] M.H. Jahanian, F. Amin, A.H. Jahangir, "Analysis of TESLA protocol in vehicular ad hoc networks using timed colored Petrinets", in: *Proc. 6th International Conference on Information and Communication Systems, ICICS-2015*, April 2015, pp. 222–227, doi:10.1109/IACS.2015.7103231
- [27] A. Studer, F. Bai, B. Bellur, A. Perrig, "Flexible, extensible, and efficient VANET authentication", *Journal of Communication and Networks*, Volume 11 Issue 6, December 2009, pp. 574–588, doi:10.1109/JCN.2009.6388411
- [28] S.S. Manvi, M.S. Kakkasageri, D.G. Adiga, "Message authentication in vehicular ad hoc networks: ECDSA based approach", in: *Proc. International Conference on Future Computer and Communication, ICFCC-2009*, April 2009, pp.16–20, doi: 10.1109/ICFCC.2009.120
- [29] R. Kalkundri, S.A. Kulkarni, "A secure message authentication scheme for VANET using ECDSA", in: *Proc. 4th International Conference on Computing, Communications and Networking Technologies, ICCCNT*, January 2014, pp.1–6, doi:10.1109/ICCCNT.2013.6726769
- [30] J.J. Haas, Y. Hu, K.P. Laberteaux, "Real-world VANET security protocol performance", in: *Proc. IEEE Global Telecommunications Conference*, March 2010, pp.1–7, doi:10.1109/GLOCOM.2009.5426188
- [31] J. Petit, "Analysis of ECDSA authentication processing in VANETs", in: *Proc. 3rd International Conference on New Technologies, Mobility and Security, NTMS*, January 2010, pp. 3–7, doi:10.1109/NTMS.2009.5384696
- [32] M. Sivasakthi and S. Suresh, "Research on vehicular ad hoc networks (VANETs): an overview", *Journal of Applied Sciences and Engineering Research*, Volume 2, Issue 1, February 2013, pp. 23–27, doi: 10.5923/j.jwnc.20130303.02
- [33] H. Moustafa and Y. Zhang, "Vehicular Networks: Techniques, Standards, and Applications", *CRC Press*, January 2009, doi.org/10.1201/9781420085723
- [34] Wenshuang Liang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie, "Vehicular Ad Hoc Networks: Architectures, Research Issues, Methodologies, Challenges, and Trend", *International Journal of Distributed Sensor Networks* Volume 2015, pp. 1-11, doi:10.1155/2015/745303
- [35] J. Harri, F. Filali, and C. Bonnet, "Mobility models for vehicular ad hoc networks: a survey and taxonomy", *IEEE Communications Surveys and Tutorials*, Volume 11, Issue 4, December 2009, pp. 19–41, doi: 10.1109/SURV.2009.090403
- [36] H. Hartenstein and K. Laberteaux, "VANET-Vehicular Applications and Inter-Networking Technologies", *John Wiley & Sons*, February 2010

Authors' Profiles



Amit Kumar Goyal has received his MCA degree with Hons. from BIT, Bhilai, India and M. Tech. in Computer Science & Engineering from Dr. APJ Abdul Kalam Technical University, Lucknow. He is pursuing Ph.D. in Computer Science & Engineering from INVERTIS University, Bareilly. Presently, he is working as Associate Professor in KIET Group of Institution, Ghaziabad. His area of interest is Wireless Communication, cryptography and network security.



Dr. Gaurav Agarwal is working as HoD Computer Science and Engineering, INVERTIS University, Bareilly. His area of research is cryptography and Network Security. He has published more than 34 papers in various International / National Journals. He is also member of ISTE, IAE, IACE. He has guided 5 M. Tech. thesis.



Dr. Arun Kumar Tripathi received the B.Sc. (Electronics) degree from Dr. Hari Gour University Sagar and M. Tech. from Dr. APJ Abdul Kalam Technical University, Lucknow in Computer Science and Engineering, He has completed Ph.D. from National Institute of Technology, Kurukshetra in the field of security in PMIPv6. He has joined KIET Group of Institution, Ghaziabad in 2003 and presently working as Associate Professor. His area of interest is Blockchain, Machine Learning, Network Security, Mobile and Wireless Communication. He has published 38 papers in various International/National conferences and Journals. He is reviewer of IEEE Access, Computing Surveys and IEEE Communications Letters. He is also member of ACEEE, IACSIT and IAENG societies.

How to cite this paper: Amit Kumar Goyal, Gaurav Agarwal, Arun Kumar Tripathi, "Network Architectures, Challenges, Security Attacks, Research Domains and Research Methodologies in VANET: A Survey", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.10, pp.37-44, 2019. DOI: 10.5815/ijcnis.2019.10.05