An Extensive Study on the State-of-the-Art Literature to Identify Major Approaches and Trust Issues of Trust-based Models in VANETs

Anurag Gupta and Anil Kumar Sagar*

Department of CSE School of Engineering and Technology, Sharda University, Greater Noida, India
E-mail: 03anuraggupta@gmail.com; aksagar22@gmail.com
**Corresponding Author*

Received 08 January 2025; Accepted 01 May 2025

Abstract

Therefore, Vehicular Ad-hoc Networks (VANETs) are the fundamental infrastructure required for the deployment of Intelligent Transportation Systems (ITS), which will facilitate enhanced safety, efficiency and comfort by interconnecting vehicles. Trust establishment is first and foremost for the smooth operation of VANETs, with trust appearing as necessary in the case for safe dissemination and preventive measures against malicious behaviours for nodes making use of inter-communication within the network. This paper provides a comprehensive summary of the existing trust-based models in VANETs, and takes an in-depth look into associated issues. We go through entity-centric, data-centric and hybrid models providing their strengths and limitations. This is backed by the statistics which indicate that implementing emerging technologies such as block chain and machine learning can greatly improve the reliability mechanisms. Moreover, they overcome the limitations suggested by trust models including dynamic network topology, scalability and problems related to privacy and security etc.

Journal of Mobile Multimedia, Vol. 21_3&4, 429–446.
doi: 10.13052/jmm1550-4646.21345

This systematic review will facilitate the insight of researchers regarding the state-of-the-art research in trust and also highlight necessary enhancements in order to produce stable and efficient models for trust in VANETs. This highlights the need for interdisciplinary teamwork in integrating cryptographic techniques, machine learning solutions, and informative messages to develop resilient trust systems against adversarial activities on vehicular communication networks.

Keywords: Vehicular ad-hoc networks (VANETs), trust-based models, intelligent transportation systems (ITS), block chain, machine learning, network security.

1 Introduction

Vehicular Ad-hoc Networks (VANETs), a subset of Mobile Ad-hoc Networks (MANETs), are specially designed to support communications among vehicles and vehicle-to-infrastructure. Their applications in Intelligent Transportation Systems – ITS – are expected to improve road safety, traffic management efficiency and passenger comfort by real-time information exchange and coordination. Due to the high mobility and frequent topology changes, VANETs require efficient design principles aimed at a fast data dissemination. In VANETs, a major challenge is to build trust among involved parties. VANETs are an open and dynamic networking environment in which several security threats and attacks may exist on the account of without deploying trust mechanisms effectively. VANET communications SOLUTIONS Trust based models. These models assess and verify the information being propagated is reliable, and certify the network nodes. Trust of VANETs can be divided into entity-centric, data-centric and hybrid trust models. The user entity writes data through the write interface, and each of its transactions are processed by a Quorum node in the system that assign a trust scores QS to bother other node and related data. A hybrid model fuses the two types for an inclusive evaluation. Novel technologies like block chain and machine learning are getting incorporated with trust models for VANETs. On the one hand, the decentralized and immutable characteristics of block chain improves transparency and trust management, while on the other side machine learning/AI provides highly sophisticated techniques to measure and predict trustworthiness across extensive data patterns. In the last hour of my paper I organize this paper as follow: The Current status of Trust-based models in VANETs will be overviewed in Section 2 which focuses on

Related Work. In Section 3, we delineate the main challenges encountered in deploying trust-based models in real VANET environments, such as dynamic network topology, scalability, as well as privacy and security issues. Section 4 outlines some points to think about for future research and also suggests approaches to overcome the current challenges. In Section 5, conclusions are drawn for the main findings of the review and contributions.

2 Related Work

V. Karanam et al. [8] The main goals of safety applications are decreasing the number of accidents and improving travel efficiency. Traffic Accident and a resulting delay on road. If there is a crash the appropriate information will need to be sent out as a broadcast message so other vehicle can change their pathways accordingly.

P. Jain et al. [9] Vehicular ad hoc network, also known as VANET is another widely popular research area. These networks where cars are represented as nodes move fast and hence high mobility wireless connections. With the automobile sector expanding like never before, it becomes necessary to have a methodized form of this for driving assistance and traffic monitoring. Deciding which node is the best to have the next one in line when connecting the starting point and its destination consists of multiple levels with increasing complexity.

Liu Qingzi, et al. [10] Butier: Recently, the security of VANET has attracted loud attentions from researchers with multiple academic backgrounds. Civil life and property protection can be achieved only if both transportation security as well as VANET throughput are maintained. Given the emphasis on the importance of addressing VANET security in our system, while there may still be vulnerabilities this architecture represents a buffer against potential threats.

Coti, R. B., et al. [11] The proposed VANET architectures contain three unique V2X cases; the first one is to transfer collected data in secure Manner-the prompt manner using a vehicle-to-vehicle (V-V), where all vehicles communicate with each other, but not necessarily via Roadside Unit an example of DSRC standard. This paper proposes a multi-agent safety information transmission approach for enhancing the V2V communication. In the proposed dissemination method, we have applied far-end node selection at out range for data forwarding with less number of transmissions. Our primary contribution to the ongoing research is designing and building significant information delivery systems with minimal end-to-end latency.

T. Diab et al. [12] The model relies on cryptographic algorithms and tunnels to use digital signatures with authentication mechanisms. We improve the security of the designed protocol in terms of data confidentiality, non-repudiation, anonymity and integrity. We show that our model is efficient and safe by describing several instances of anonymity with performance results. Our simulations have been launched on the NS3 platform.

3 Trust-Based Models in VANETs

The VANET System Components package includes essential entities like Vehicle Nodes, Roadside Units (RSUs), Centralized Authority, and User Devices, highlighting their roles in data communication and interaction within the network. The Trust Management Framework consists of components like Trust Evaluation, Trust Update Mechanism, Trust-based Decision Making, and Trust Information Database, which collectively manage and update trust metrics for effective decision-making. Additionally, the Communication Security Layer encompasses Secure Communication Protocol, Data Authentication, Encryption Mechanism, and Data Integrity Check, ensuring that communications within the VANET are secure and reliable [18]. The connections between components illustrate the flow of data and trust assessments, ensuring that reliable feedback is provided to vehicles and users. This structured approach facilitates enhanced security and scalability in VANETs, essential for safe and efficient vehicular communication.

3.1 System Architecture for Trust-Based Models in VANETs

In Trust Based Models for System Architecture in VANETs, the authors present several important components to be considered while implementing a system architecture that collectively contributes towards receiving reliable and secure information together with an assurance that vehicular communication can result in efficient results. The Trust-Based Models module is the heart of our architecture implementing models to deal with different trust concerns in a VANET. It is further broken down into: Entity-Centric Models, Data-Centric and Hybrid trust models which concentrate on different aspects related to the management of trusts. Entity-centric models [16] serve as a basis for how the trustworthiness of individual vehicles or “entities” in your network will be measured. Reputation-Based Trust and Behavior Based-Trust These models are dependent on relations one has with others as well as the other people have seen how we operate to make conclusion about our trust

levels. Reputation-Based Trust is founded on trust that arises when many other nodes give positive feedback regarding a node entity past behavior, and Behavior-Based Trust is based on the monitoring of behaviors (actions) over time in real-time from potentially anomalous actors. This guarantees that just vehicles with demonstrated conformance may participate on the network, improving safety at all. Meanwhile, Data-Centric Models address the data-awareness of network messages exchanged between them. These are built

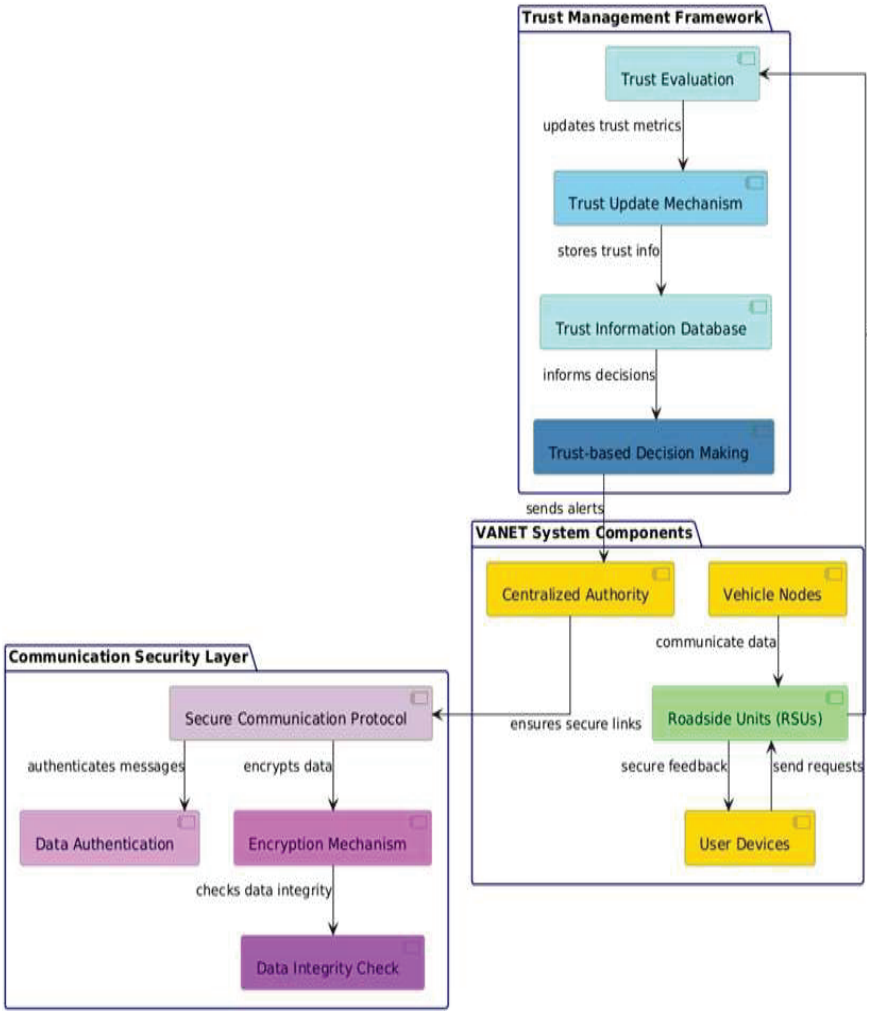

Figure 1 System architecture for trust-based.

to prevent data being altered in transfer, and make sure both you and your customer is getting accurate information [17] from a credible source.

Data Authentication validates the information source and correctness which is important for accurate QoS traffic control, and Message Integrity Verification uses cryptographically methods to detect if messages have NOT been mangled with.

3.2 Types of Trust-Categories

In the Trust Categories section, models such as Reputation-Based, Feedback-Based, Certificate less, and Context-Aware trust are presented, each visually differentiated by distinct colors to enhance clarity. This categorization highlights the different approaches to establishing trust among vehicles and roadside units. The Assessment Mechanisms package details how trust is evaluated, featuring methods like Direct Assessment, Indirect Assessment, Hybrid Assessment, and Dynamic Assessment, which underline various strategies to gauge trustworthiness based on direct experiences, peer feedback, or a combination of both. Lastly, the Update Methods section encompasses trust maintenance techniques, such as Continuous Update and Event-Driven Update, indicating how trust metrics are regularly revised to adapt to changing conditions. Overall, this diagram provides an intuitive

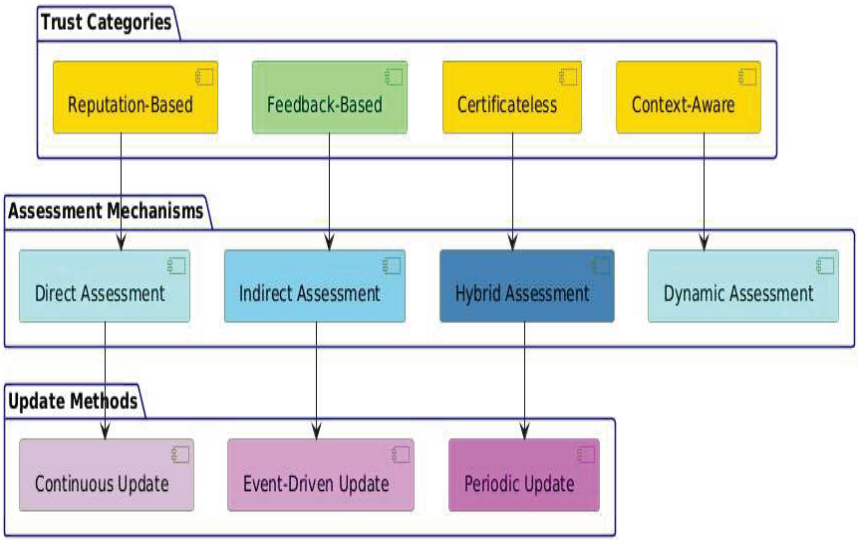

Figure 2 Types of trust-categories in VANETs.

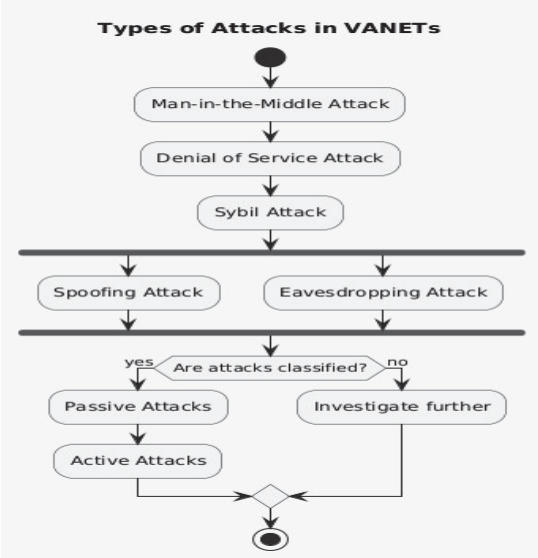

Figure 3 Types of attacks in VANETs.

understanding of trust management in VANETs, which is crucial for ensuring secure and reliable communication in intelligent transportation systems.

3.3 Types of Attacks in VANETs

VANETs (Vehicular Ad-hoc Networks) are dynamic and completely isolated networks in which vehicles can communicate with each other as well as roadside infrastructure to improve the overall traffic efficiency, safety, and provide information services. There are several attacks possible on VANETs because, despite their advantages and extensibility in terms of services provided by them, these networks also possess many threats which can threaten their performance, security and reliability. We need to know about these attacks for developing efficient security strategies that secure the VANETs from abnormal activities. Sybil Attack is one of the most popular attacks in VANETs. In such an attack, a single malicious vehicle generates.

3.4 Machine Learning-Based Techniques in VANETs

Recently, machine learning (ML) techniques have shown great potential in mitigating new challenges arising due to the dynamic and complex nature of Vehicular Ad-Hoc Networks (VANETs). Data-driven methods combined

with machine learning (ML)-based technologies increase effectiveness, reliability, and scalability of VANETs by supporting the decision-making process through advanced processing techniques based on data analysis for traffic prediction detection, anomaly detections or network optimization. The following section discusses pertinent machine learning techniques used in VANETs, and how they are integrated into the network for improved performance.

1. **Security and Anomaly Detection**
   Security is one of the most important challenges in VANETs since they are open, and distributed systems. Its security is improved by employing the ML techniques such as anomaly detection and intrusion prevention.
2. **Vehicle Behavior Modeming**
   In VANETs, ML techniques are used to model and predict vehicle behavior as well.
3. System Optimization / Resource Allocation and Traffic orchestration
   High performance of VANETs is characterized by efficient resource allocation and network optimization.
4. **Context-Aware Services**
   The context-aware services in VANETs must receive and process the contextual knowledge of vehicles and infrastructure. These contextual factors include location, speed and environmental conditions;
5. **Recommendation Systems with Collaborative Filtering**
   In VANETs, formats that adopt collaborative filtering and recommendation system to serve user with customized services are used as a medium. In this study, ML techniques in the form of Matric Factorization.

3.5 Blockchain-Based Techniques in VANETs

Initially being practiced in cryptography because of cryptocurrency transactions, the blockchain technology has been instigated into other sectors and areas with it having its purposeful application to Vehicular Ad-hoc Networks (VANETs) Given its characteristics of being decentralized, transparent and immutable it makes even more sense to use blockchain for solving many issues in the automotive field including VANETs. To secure VANETs, this section addresses the use of blocking technology and describes how implementing it impacts the security improvements in network: – defines mechanisms over data integrity control and management.

1. **Enhanced Security and Trust**
   Some of its key advantages in VANETs are improved security and trust by the network participants using blockchain technology. VANETs

are characterized by open and decentralization but also susceptible to numerous attacks such as Sybil attack, Jamming/Spoofing, Data tampering in traditional VANET.

2. **Hexolab: Communication Security and Information Sharing**
   The secure exchange of information and data between road vehicles, roads authorities (and their structures), or any kind of fixed infrastructure are made possible by blockchains. Vehicles must share information about traffic conditions, road hazards or safety warnings in VANETs
3. **Self-sovereign Identity Management**
   One of the essential applications of blockchain technology is decentralized identity management in case of VANETs. Centralized authorities that manage these identities are fallible and easily hacked or breached. The self-sovereign identity is the idea that my personal data are mine and untouchable from any other people or entities, then can we make it a thing?
4. **Efficient Resource Management**
   Blockchains help in better management of resources which VANETs require to function efficiently. It offers the ability for network resources to be tracked and managed through decentralized party service providers using blockchain technology.
5. **Auditability of Data along the data lineage.**
   Thus, because of the immutability and transparency that blockchain provides, we believe it can be useful for providing data provenance and audit capabilities in VANETs.

3.6 Algorithm

Algorithm: GENERALVANETOPERATION(V, P, T, R)

Input:

- $V = \{v_1, v_2, \ldots, v_n\}$: Set of vehicles
- P: Set of packets/messages to be transmitted
- T: Trust parameters and evaluation function (optional)
- R: Routing protocol or rules

Output: Reliable message delivery and updated trust states

1. **for each** vehicle $v_i \in V$ **do**
2. Initialize communication interfaces and buffers
3. Determine neighbors within communication range
4. **for each** message $p \in P$ generated by v_i **do**
5. Select next-hop vehicle v_j based on routing protocol R
6. Transmit p to v_j
7. **if** acknowledgment not received **then**
8. Retry or select alternate route
9. **end if**
10. Log interaction outcome (success/failure)
11. **if** trust model is enabled **then**
12. Update trust score $T_i(v_j)$ based on interaction
13. **end if**
14. **end for**
15. Periodically broadcast beacon or hello messages
16. Update neighbor tables and network topology
17. Respond to received messages or alerts
18. Apply security rules or intrusion detection if applicable
19. **end for**

General VANET Operation algorithm models the core functioning of a Vehicular Ad-Hoc Network (VANET), outlining how vehicles dynamically communicate and route messages in a decentralized environment. Each vehicle initializes its communication module, discovers neighbouring nodes within range, and prepares to exchange messages. For every packet generated, the vehicle selects a next-hop neighbour based on a routing protocol (e.g., GPSR, AODV), attempts transmission, and handles failures via retries or alternate paths. These steps ensure that the highly dynamic and mobile nature of VANETs is accommodated through continuous message relaying and adaptive routing strategies.

Additionally, the algorithm supports optional trust evaluation, enabling vehicles to assess the reliability of neighbours based on past interactions. This is useful for detecting and mitigating malicious behaviour or routing failures. Vehicles periodically send beacon messages to maintain up-to-date neighbour tables and network topology. They also respond to received messages or alerts and may integrate security mechanisms like intrusion detection. Overall, the algorithm captures both communication and decision-making aspects of

VANETs, forming a foundation upon which advanced features such as trust models, security protocols, or machine learning-based optimization can be built.

3.7 Challenges in Trust-Based Models for VANETs

Vehicular Ad-hoc Networks (VANETs) – which are the sub-set of Mobile ad hoc networks(manet)are a new and promising paradigm in automotive technology that allow vehicles to communicate real-time information between them as well as with the roadside infrastructure [22]. Central is trust based models that are responsible for the network's reliability, security and efficiency. On the one hand, VANETs need efficient trust-based mechanisms to add transparency and robustness most of its applications but on other side these models also suffer from numerous challenges during their implementation and operation. The dynamic nature of VANETs, the open environment in which they are deployed and a constantly changing threat landscape all play into these challenges.

1. **Dynamic Network Topology**
   The highly dynamic nature of the network topology represents one of the main challenges for VANETs. Since vehicles move in and out of the network constantly, this represents a fluid environment (vehicles will join and leave at any time). The dynamism of trust models makes it hard to provide current and accurate assessments.
2. **Scalability Issues**
   Another significant issue regarding trust-based models in the context of VANETs is Scalability. The increase in the number of vehicles and infrastructure nodes will ultimately raise the problem complexity regarding trust management and evaluation.
3. **Security and Privacy Concerns**
   Trust-based models that could be proposed to assemble the trust in VANETs should maintain their efficiency as well as deal with security and privacy issues, since this can solve efficiently the traditional "byzantine fault" problem. Trust needs to be able to handle all kind of attacks, including but not limited Sybil-attacks – where a single malicious node pretends their many nodes and Collusion attack – when multiple bad-eyed trust proofers work against the system.
4. **Data Integrity and Accuracy**
   Data integrity and accuracy is utmost important in trust-based models of VANETs. The fidelity of the trust model relying on true data to

determine a level of trust. Mistakes based on data inaccurate or incomplete can create false confidence ratings causing the entire network to be thrown into controversy.

5. **Resource Constraints**
   Vehicular Ad Hoc Network (VANET) is built by vehicles that are equipped with limited computational resources such as processing power, memory and energy. Trust-based models have to comply with these limits and at the same time provide meaningful trust evaluations.
6. **Adapting to Evolving Threats**
   Moreover, the VANET threat landscape remains dynamic in nature and new attack vectors may not only keep on emerging but colluding methods are being developed concurrently. If trust is the foundation of this model, it follows that as the threats change so should how we provide these types of services.

4 Future Research Directions in Trust-Based Models for VANETs

As problems have arisen and new technologies have been developed in Vehicular Ad-hoc Networks (VANETs), the field of trust-based models is rapidly growing to help researchers and practitioners address them. Research directions are critical to enhancing the effectiveness, reliability, and security of trust-based models. Key areas of interest include the development of new methodologies and integration techniques, scalability issues, and addressing anomalies at the intersection of theory, design, and implementation.

5 Conclusion

It is quite up to the mark that trust management model shows some considerable challenges to achieve success in vehicular communication system especially in the case of VANETs. Trust needs are changing fast, given the rapid pace of change in automotive technology, so new solutions for trust have become an urgent requirement. These traditional trust models do not work very well in VANETs, as they assume that trust in the network is static and thus ignored mobility aspect of nodes in a particular technology domain unlike other portable networks. The blockchain technology with the help of machine learning, and NLP methods can help in improving trustworthiness reliability through a dynamic analysis of emerging patterns

over extensive datasets. These are big challenges to integrate, especially as vehicle and data traffic continue to scale up. These frameworks should be scalable and may have many decentralized components with cryptographic protocols to manage trust and provide privacy and security. But theory needs to be checked and adjusted in practice. In order to close the chasms and transform the trust models to feasible mechanisms, it is important that these are tested and integrated with our partners from industry. Future research should concentrate on developing adaptive trust models that deal with the complex and inter-domain nature of VANETs.

References

[1] M. Syfullah and J. M. -Y. Lim, "Data broadcasting on Cloud-VANET for IEEE 802.11p and LTE hybrid VANET architectures," 2017 3rd International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad, India, 2017, pp. 1–6.

[2] Z. Yang, K. Yang, L. Lei, K. Zheng and V. C. M. Leung, "Blockchain-Based Decentralized Trust Management in Vehicular Networks," in IEEE Internet of Things Journal, vol. 6, no. 2, pp. 1495–1505, April 2019, doi: 10.1109/JIOT.2018.2836144.

[3] P. Kohli, S. Painuly, P. Matta and S. Sharma, "Future Trends of Security and Privacy in Next Generation VANET," 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Thoothukudi, India, 2020, pp. 1372–1375, doi: 10.1109/ICISS49785.2020.9316043.

[4] P. Surasura and J. G. Naragund., "Analysis of Highway Routing Protocols for VANETS," 2022 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), Bangalore, India, 2022, pp. 1–7, doi: 10.1109/SMARTGENCON56628.2022.10084195.

[5] Rasheed Hussain, Fatima Hussain, and Sherali Zeadally. 2019. Integration of VANET and 5G Security: A review of design and implementation issues. Future Generation Computer Systems 101, 2019, 843–864. doi.org/10.1016/j.future.2019.07.006.

[6] G. Kaur, M. Khurana and A. Kaur, "Gray Hole Attack Detection and Prevention System in Vehicular Adhoc Network (VANET)," 2022 3rd International Conference on Computing, Analytics and Networks (ICAN), Rajpura, Punjab, India, 2022, pp. 1–6, doi: 10.1109/ICAN56228.2022.10007192.

[7] R. Sultana, J. Grover and M. Tripathi, "A Novel Framework for Misbehavior Detection in SDN-based VANET," 2020 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), New Delhi, India, 2020, pp. 1–6, doi: 10.1109/ANTS50601.2020.934277.

[8] V. Karanam, B. U. Maheswari and T. S. B. Sudarshan, "Overlay based fault tolerant peer to peer multicasting for emergency data communication in VANETS," 2017 International Conference On Smart Technologies For Smart Nation (SmartTechCon), Bengaluru, India, 2017, pp. 510–513, doi: 10.1109/SmartTechCon.2017.8358425.

[9] P. Jain and D. Arora, "Fuzzification based intravehicular communication in VANETs," 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2017, pp. 223–228, doi: 10.1109/I-SMAC.2017.8058344.

[10] Qingzi Liu, Qiwu Wu and Li Yong, "A hierarchical security architecture of VANET," International Conference on Cyberspace Technology (CCT 2013), Beijing, China, 2013, pp. 6–10, doi: 10.1049/cp.2013.2080.

[11] R. B. Koti and M. S. Kakkasageri, "Intelligent Safety Information Dissemination Scheme for V2V Communication in VANETs," 2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2019, pp. 1–6, doi: 10.1109/ICSCAN.2019.8878862.

[12] T. Diab, M. Gilg, F. Drouhin and P. Lorenz, "Anonymizing Communication in VANets by Applying I2P Mechanisms," 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1–6, doi: 10.1109/GLOBECOM38437.2019.9013225.

[13] R. Bala and C. R. Krishna, "Scenario Based Performance Analysis of AODV and GPSR Routing Protocols in a VANET," 2015 IEEE International Conference on Computational Intelligence & Communication Technology, Ghaziabad, India, 2015, pp. 432–437, doi: 10.1109/CICT.2015.54.

[14] Zheng Wei, Xiangyu Bai and Yankun Feng, "Cooperative download mechanism of vehicle communications on the highway vanet," 2014 International Conference on Information and Communications Technologies (ICT 2014), Nanjing, China, 2014, pp. 1–6, doi: 10.1049/cp.2014.0587.

[15] D. B. Rawat, B. B. Bista and G. Yan, "CoR-VANETs: Game Theoretic Approach for Channel and Rate Selection in Cognitive Radio VANETs," 2012 Seventh International Conference on Broadband,

Wireless Computing, Communication and Applications, Victoria, BC, Canada, 2012, pp. 94–99, doi: 10.1109/BWCCA.2012.26.

[16] K. Sundari and A. Senthil Thilak, "Impact of realistic mobility models on the performance of VANET routing protocols," 2023 International Conference on Signal Processing, Computation, Electronics, Power and Telecommunication (IConSCEPT), Karaikal, India, 2023, pp. 1–6, doi: 10.1109/IConSCEPT57958.2023.10170053.

[17] P. Boonnithiphat and Y. Somchit, "New cost calculation method for finding shortest path of Hybrid VANET protocol," 2016 International Computer Science and Engineering Conference (ICSEC), Chiang Mai, Thailand, 2016, pp. 1–6, doi: 10.1109/ICSEC.2016.7859931.

[18] Narechania, A. Karduni, R. Wesslen and E. Wall, "VITALITY: Promoting Serendipitous Discovery of Academic Literature with Transformers & Visual Analytics," in IEEE Transactions on Visualization and Computer Graphics, vol. 28, no. 1, pp. 486–496, Jan. 2022, doi: 10.1109/TVCG.2021.3114820.

[19] M. Alkubeily, S. A. Sakulin and B. Hasan, "Design an Adaptive Trajectory to Support UAV Assisted VANET Networks," 2023 5th International Youth Conference on Radio Electronics, Electrical and Power Engineering (REEPE), Moscow, Russian Federation, 2023, pp. 1–6, doi: 10.1109/REEPE57272.2023.10086859.

[20] R. Bhakthavathsalam, S. Nayak and M. G. Srikumar, "Expediency of penetration ratio and evaluation of mean throughput for safety and commercial applications in VANETs," 2009 International Conference on Ultra-Modern Telecommunications & Workshops, St. Petersburg, Russia, 2009, pp. 1–5, doi: 10.1109/ICUMT.2009.5345426.

[21] I. Naqvi, A. Chaudhary and A. Rana, "Intrusion Detection in VANETs," 2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2021, pp. 1–5, doi: 10.1109/ICRITO51393.2021.9596141.

[22] D. Gutierrez-Rojas, P. H. J. Nardelli, G. Mendes and P. Popovski, "Review of the State of the Art on Adaptive Protection for Microgrids Based on Communications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 3, pp. 1539–1552, March 2021, doi: 10.1109/TII.2020.3006845.

[23] S.A. Soleymani, A.H. Abdullah, W.H. Hassan, M.H. Anisi, S. Goudarzi, M.A.R. Baee, S. Mandala, "Trust management in vehicular ad hoc

network: a systematic review", EURASIP Journal onWireless Communications and Networking, 2015.

[24] Narechania, A. Karduni, R. Wesslen and E. Wall, "VITALITY: Promoting Serendipitous Discovery of Academic Literature with Transformers & Visual Analytics," in IEEE Transactions on Visualization and Computer Graphics, vol. 28, no. 1, pp. 486–496, Jan. 2022, doi: 10.1109/TVCG.2021.3114820.

Biographies

Anurag Gupta received the bachelor's degree in Information Technology from Anand Engineering College, Keetham Agra in 2009, the master's degree in computer science and engineering from Galgotias College of Technology and Management, Greater Noida in 2015, and Pursuing the philosophy of doctorate degree in Computer Science and Engineering from Sharda University, Greater Noida, respectively. His research areas Ad-hoc Networks.

Anil Kumar Sagar is currently working as Professor & Head of Department of Computer Science Engineering in School of Engineering and Technology, Sharda University, India. Dr. Anil Kumar Sagar obtained his doctorate from JNU, New Delhi in the area of Ad-hoc Networks. He obtained his B.E-Computer Science & Engineering from G B Pant Engineering College Pauri

Garhwal, and M.Tech from JSSATE Noida. Formerly served as a Dean Academics in Raj Kumar Goel Institute of Technology Ghaziabad. He also worked as a Member of Board of Studies in Computer Science Department at Galgotias University Greater Noida and RKGIT Ghaziabad. He is a Member in editorial board/review committee in many international/national journals and served as a program/organizing committee member for organizing several conferences. Guided 10 M.Tech (Computer Science) students and presently guiding 5 Ph. D. (Computer Science) students. He is having about 20 yrs. of teaching experience in various prestigious colleges and universities.