ISSN 2278-3091
Volume 8, No.4, July – August 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse83842019.pdf
https://doi.org/10.30534/ijatcse/2019/83842019

An Empirical Study on Issues Challenges Tools and Techniques of Vehicular Ad-Hoc Network Communications

D.N.S. Ravi Kumar[1], Dr.S. Barani[2]
[1]Research Scholar, Sathyabama Institute of Science & Technology
[2]Professor, Sathyabama Institute of Science & Technology

ABSTRACT

By the explosive development of mobile traffic demand, the conflict among capability necessities and spectrum unavailability turn out to be progressively protruding. Vehicular communication is categorized by a dynamic atmosphere, comparatively low, and high mobility antenna heights on the (vehicles and roadside units) interactive units. These features create the vehicular broadcast and channel forming predominantly a challenging one. VANET collects and allots safety information's so as to minimalize the sum of accidents on a huge scale. The information is composed from the antennas on the vehicles that can be interrelated to drivers on street. It is very demanding to found and reserve endwise networks in a Vehicle Ad-Hoc Network (VANET) as a consequence of high vehicle speed, extended inter-vehicle distance and fluctuating vehicle density. This survey aims at analyzing the advantages and limitations of various existing approaches.

Key Words : Vehicle Ad-Hoc Network ,roadside units, vehicle density

1. INTRODUCTION

The past decade has perceived the increase of a wireless communication information that assurances to expand the traveling experience on roads. Vehicles and [1-3]road-side-units (RSUs) with detecting abilities are now competent to gather data about the traffic and road conditions with remarkable part and ubiquity. As the motor industry purposes to provide vehicles with the Dedicated Short Range Communication (DSRC) technology, we may shortly practice amenities of a supportable Intelligent Transportation Systems (ITS) with an intention to create traveling comfortable, safer and ecologically approachable. Internet of Vehicles (IoV) can be perceived as a superset of VANET. It covers VANET's measure, organization and uses. Altered from outdated (ITS) Intelligent Transportation System, it places more importance on data communication among humans, vehicles and roadside units (RSU). Its objective is to create individuals expansion of actual road traffic data simply, to [4-9]safe guard the travel suitability, and to progress the comfort of travel. As a significant division of IoV, Internet of Things is mostly utilized in metropolitan road traffic atmosphere to offer system admittance for passengers, traffic management personnel, and drivers. IoV location is the arrangement of wireless network location and road environments. Irregular road traffic circumstances and the active topology of the system can be stimulating for the appropriate distribution of the communications. However VANETs grants a [10-13]distinctive kind of encounters for transmitting, conversely it correspondingly grants resolutions via clustering procedures. Clustering can be valuable in conserving the reliability and stability of an ad-hoc system that effects in performance improvement. Clustering is essentially a significant tools in VANET that overtake the MANET clustering procedures alike lowermost ID process, maximum grade process etc. that does not accomplish well on the field of VANET. In addition to the importance of vehicular ad- hoc systems, they have a virtuous influence in mishap prevention, information dissemination, congestion detection etc. The safety contents by RSU utilizes On-Board Units (OBUs) with geographical maps commonly referred as popular content distribution. Peer-to-Peer (P2P) protocols have been employed to download various multimedia services to support efficient Persistence Contrastive Divergence (PCD). The adaptation of P2P ideas to construct an efficient V2V communication in VANET usually consumes less than one minute. However, download of a large file by the OBUs within the duration of one minute is impossible and hence monitoring of packet exchange amongst the OBUs is necessary for the following scenarios. Intelligent Transport Systems use communication knowledge's [14-18]to deal actual road traffic data facilities to highway workers and administration executives. Vehicular Ad Hoc Networks is a significant constituent of ITS wherever vehicles interconnect by other vehicles and road-side structures, examine and development established data, and create resolutions conferring to that.

2. STANDARDS FOR WIRELESS ACCESS IN VANET

[20] elucidated a road safety applications using VANETs (figure 1) for enhancing the safety measures while driving in terms of broadcasting the messages. In this work, the capability of the current wireless technologies were discussed for providing reliable safety messages broadcast, that are essential in road safety application. In different high way and city scenarios, the presentation of IEEE 802.11p standard was associated with VeMAC protocol via computer simulations as well as a traffic blockage situation created with the emergency space of a motor vehicle on a freeway. In this approach the current VeMAC protocol was discussed together with prototype experiments.

[19] presented a challenges that are faced by the VANET and the security framework was also discussed in this approach. A three parts of security frameworks and its challenges and requirements have also been discussed. To assist the secure VANET infrastructure with effectual communication amongst parties, some of the requirements should be considered. And also the current security architectures and famous security standards of protocols were discussed. The different attacks were also taken into consideration. Finally comparison was also made for acquiring solution related to well-known security strategies.

[18] elucidated a current development over wireless communication technologies and automobile industry. It was generated an important investigation attention in the VANETs in the preceding limited existences. Vehicular Network comprised of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications continued through wireless access technologies like IEEE 802.11p. In wireless communication, the innovation have been expected for enlightening highway security and motorized road traffic competence in upcoming over the growth of (ITS) Intelligent Transport Systems. Therefore, for launching standard VANET, administration auto-mobile trades and academic world were severely accompanying via numerous research projects. The VANET characteristic set application areas like vehicle accident cautionary and road traffic data distribution have prepared VANET an fascinating arena of mobile wireless communication. Thus the potentials of VANETs was also analyzed and also the customs to achieve long awaited ITS was discussed.

[21] elucidated a current research of VANET application area. More number of vehicles were fortified by means of embedded sensors. It created a countless prospects to make an influential and possible life-changing solicitations on security, comfort, competence, public association and contribution, when they are available on the highway. Even though, greatly measured different cases of mobile ad hoc network was considered, the controlled mobility of vehicles brought various challenges in data message and solicitation strategy of VANETs. Because of extremely dynamic and sporadic linked topology and diverse request's QoS necessities, the problems were occurred. Thus the protocol stack type have also been discussed and made comparison among utmost common proto-cols. Many problems were discussed to improve the design of VANET to meet the specific requirements.

[22] suggested a scalable and cooperative medium access control (MAC) protocol to overcome the conventional method issues such as SDMA based protocols that requisite for the digital map updating, which was not convenient and cost effective as well. In order to realize the reliable and scalable periodic beaconing for VANETs, SCMAC was designed. SCMAC afforded simple and cost effective when compared to cluster-based or SDMA-based protocols. The CCH can be reutilized in TDMA. Using cooperative beaconing the upcoming CCH condition was well-versed among nodes. The slot access method was designed on the basis of cooperative beaconing. The collisions were suppressed through random selection policy for enhancing reliability. A beaconing period should be sustained that matches the current node density for supporting scalability. The great potential node density conditions were considered in VANETs, the idle slots has to be prepared by applying proactive slot reservation policy for joining the new nodes at any time. Also, SCMAC satisfied severe delay restraint when there is fewer node density. Thus it was verified with the experimental approaches.

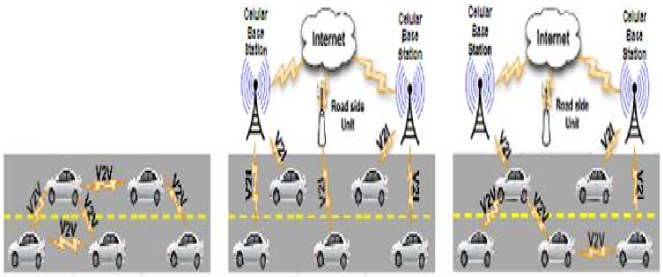

Figure 1: Structure of VANET

3. VANET APPLICATION

[23] elucidated a framework in the simulation models which is precise in vehicular communication. In this approach, the flat of applicability and granularity of IVC applications were also discussed. The most broadly used reproduction structures like Veins, temporarily offers all the mechanisms and prototypes desired for presentation assessment of vehicular networking procedures and uses – besides that is equivalent to perfect setups thoroughly.

[24]An ad hoc network comprising of vehicles has appeared as a thought-provoking however inspiring area wherever a portion of different use might discover their place. Although investigation in this arena is on meanwhile preceding two years, extensive real-world application still have need of some interval. The foremost determination of traffic control and managing uses is to enhance traffic movements and to diminish the transportable period by evading road traffic crowding or support the driver about preeminent direction with efficient road circumstances. This can include the usage of some roadside equipment, e.g., smart traffic signs and e-sign boarding. Data about the highway blockings onward can certainly aid in decreasing the crowding and enlightening the volume of transportations.

[25] suggested the application of VANET and its challenges. VANET is fetching a dynamic part of study as it has wonderful prospective to develop security of vehicles and traffic competence. We custom the VANET in its place of Mobile Ad hoc Network (MANET) because of great flexibility of the vehicles as MANET ensures not to upkeep high mobility. Wireless Vehicular ad hoc network tools is intended for permitting wireless message among vehicles on the road, allowing the transmission of data to safeguard heavy security and road traffic administration by internet admittance to drivers and systems analyst. VANET applications comprise payment services, location-based services, infotainment, and traffic optimization. On condition that safety in VANET is a thought-provoking because of its features alike:

- System topology variations,

- Wireless communication,
- High mobility,
- Absence of infrastructure Storage capacity,
- Frequent exchange of information,
- Limited bandwidth,
- Battery power and
- Scalability.

[26] presented a description regarding the application of VANET. Gradually vehicles are actually well-found by entrenched devices, dispensation besides wireless communication competences. This devours released a countless of potentials for influential and possible uses on efficiency, safety, public collaboration, participation, and comfort whereas they are proceeding the highway. Though, measured as a different circumstance of a Mobile Ad Hoc Network, the great however embarrassed flexibility of vehicles carry new contests to data application and communication policy in VANETs. This is owing to their greatly active and alternating linked topology and dissimilar application's QoS necessities.

4. SECURITY ISSUES

[27] presented a novel privacy preserving schemes in ad hoc social networks with mobile social networks (MSNs) and vehicular social networks (VSNs). The thirty three privacy preserving schemes were examined specifically. According to its existing privacy preservation schemes, the privacy preserving models were reviewed. And also, an outline of recommendations was also provided. From this survey, the readers could have capability for comprehensive understanding of research trends over privacy-preserving systems for ad hoc social networks.

[28] Elucidated an intrusion detection system in cluster based approach intended for storage area network. A storage area network SAN was broadly employed special drive network that linked a various types of storage devices with related data servers for a larger network of users. IDS Intrusion detection system was a security mechanism hired to protect and daunt intrusions. IDS was characterized in three types

- Host based IDS which exist in the host that needed a protection against attacks.
- Network based IDS which was centralized and observed the whole network.
- Hybrid based IDS used two approaches, Firstly Rule based approach in which the pre-determined rules of what was considered as an authentic act. The procedures stood unmistakably and clearly stated and made before the actual intrusion detection process. Second an anomaly based approach, to perceive any nonconformity from the expected behavior, users or process performance were verified in contradiction of a standard profile.

In this Intrusion detection system with clustering, a same data objects were grouped on the basis of their conduct by using K-means clustering. In the K means clustering methods, an input dataset was partitioned as K clusters according to its initial value that defined as seed opinions in each clusters centroids. By using Euclidean distances method, each input data assigned towards the nearby centroid. New centroids were produced for individual cluster by computing the mean standards of the input set allocated for every cluster and the process was frequently repetitive until the results touched the convergence.

4.1 Empirical study on issues challenges tools and techniques

[29] elucidated most appropriate vehicular propagation and channel models for evaluating the protocols and also its applications. Initially, the models were classified on the basis of propagation mechanisms that employed and approach of implementation. Similarly, based on the implemented channel properties models were classified. In this approach, important attention was given for the models usability, scalability, complexity of implementation and the input requirements to analyze the better models. In this vehicular channel modeling, a fewer-explored aspects were discussed with modeling particular environs (e.g., ,overpasses, tunnels, parking lots) and communicating vehicle types (e.g., public transportation vehicles, scooters). Before the deployment, an accurate evaluation of vehicular protocols and application with suitable channel model was critical. At last, the guidelines has been offered to choose an appropriate channel model reliant to kind of protocol/application beneath evaluation, offered geographical information, and time constrictions concerning execution in simulation.

[30] Presented a new innovative approaches in VFC paradigm and its potential capability and the open issues were also discussed. The four types of scenarios were taken into consideration specified as retaining moving and parked vehicles as infrastructure for communication and computation, correspondingly. On the other side, as communication infrastructures in moving and parked vehicles supports greater ability of flow because of development in packet delivery delaying and the improved links between vehicles. For achieving better communication, the predictable moving patterns were employed among the vehicles. The computational resources of each and every vehicle was utilized through the moving and parked vehicles as computational infrastructures. In the approach, incredible computational potentialities was exploited through separating the individual vehicle resources. This survey helps to provide better guidelines for future work of vehicular system.

[31] elucidated the novel goal for providing an inclusive survey on the adaptive beaconing to start new initiation for proposals. The main motivation of this work was to analyze the capabilities of beaconing approaches with the help of significant parameters. In this work, the beaconing anatomy was described through schematic layered design and multi-channel communication viewpoint.

The design based taxonomy was introduced for categorizing the beaconing approaches. In this survey the beaconing capabilities was evaluated with significant parameters and its salient features were analyzed for highlighting key observations.

Table 1: A survey on VANET

Author and year	Network model	Privacy model	Goal	Advantage	Disadvantage
[34]	A distinctive location based services in VANET	Forward secrecy ; Backward secrecy ;Collusion resistance	Support a privacy preserving Authentication in the vehicle-user joining phase ; Enable vehicle users to separately update the session key	Key update ratio	Key update delay Compared only with the traditional key update
[35]	VANET with a group of social spots	Privacy in location	Ease vehicles to realize high level location	Feasibility is showed using Game theoretic techniques, Location privacy gain	Anonymity set size - Limited analysis with the threat model
[36]	VANET containing more number of parking spaces	Conditional privacy preservation	Improve an intelligent parking for huge parking slots ; Provision a privacy preserving of the drivers	Intelligent parking scheme	Searching time delay No comparison with other scheme in term of coverage ratio
[37]	VANET	Identity privacy preserving Traceability	In a distributed Manner guide vehicles to preferred destinations. Support a privacy preserving of the drivers	Analysis on time complexity, distributed guidelines	Processing delay Reduction in travelling time Limited analysis with the threat model
[38]	VANET	Identity privacy preserving Traceability	Solving the issues of authentication and privacy in VANET	Authentication is high	Storage requirement and computation threat model is not presented
[39]	VANET	Identity privacy preserving ; Traceability ; Revocability	Gratify the privacy requirement based only on two shared secrets	High privacy	Data transmission Worthless batch successful rate No consideration on Location privacy
[13]	VANET	Anonymity	Support a privacy preserving of broadcast message	Efficient method	Average link layer delay Average data packet delay -Location privacy is not considered
[40]	VANET with a member manager	Multi-level anonymity	Support a multilevel conditional privacy preserving	Stability is high	Storage requirements Computational overheads Limited analysis with the threat model
[41]	VANET with a social degree of an intersection vertex	Conditional privacy preservation	Enhancing vehicular DTN with RSU assistance ; Fighting privacy related attacks on vehicle DTN nodes ;	Attaining conditional privacy preservation	Packet average delay Limited consideration of routing requirements Average delivery ratio
[42]	VANET with not include RSUs	Identity privacy ; Location privacy ; Interest privacy	Ease vehicles to communicate the common interest ;	Keeps the interest privacy from other vehicles who don’t have the same interest	Average delay for finding the like-minded vehicle Limited analysis with the threat model
[27]	VANET with a collection of social spots	Receiver-location privacy	Achieving the location privacy	Sacrificing the Plum Tree for the Peach Tree” tactic	Average packet delivery ratio Average packet delay No comparison with other protocols
[43]	VANET with a collection of social spots (including small social spot and large social spot)	Location privacy ; Anonymity	Achieving the location privacy based on pseudonyms changing technique	Privacy is high	Anonymity set size No comparison with other methods
[44]	VANET with a collection of social spots	Location privacy Vehicle conditional privacy preservation	Achieving receiver location Privacy preservation in VANETs	High privacy	Average delivery ratio Packet average delay No comparison with other protocols

Author and year	Network model	Privacy model	Goal	Advantage	Disadvantage
[45]	VANET	Backward privacy; Conditional anonymity; Nonrepudiation ; Identity revocation	Solving the issues Of authentication and privacy in VANET	Authentication overhead Efficient compared to other schemes	Revocation overhead Certificate updating overhead Location privacy is not considered
[46]	VANET	Conditional privacy preservation Anonymity	Resolving the issues of authentication and privacy in VANET such	low pseudonym generation latency, high scalability, and relaxed revocation	Protocol latency analysis Comparison of search times for revocation - Mobility models are not considered
[47]	VANET with a lite certificate authority	Location privacy ; Anonymity	Solving the issues of authentication and privacy in VANET	Authentication and privacy is high	Encryption cost comparison Computational cost comparison Limited consideration of Routing protocols.
[48]	VANET with data center and a collection of social spots (including Global Social Spot and Individual Social Spot)	Location privacy	Exploit the meeting opportunities for pseudonym changing ; Improve the location privacy Preservation	Location privacy is improved	Global pseudonym entropy of the entire VSN Predictable and actual pseudonym entropy of a target vehicle Comparison with existing schemes Analysis with the threat model Many molds wanted to understand implementation
[49]	VANET with a centralized authority	Interest privacy	Protects the interest privacy from other vehicles who don't have the same interest	Privacy is highly protected	Communication overhead Limited analysis with the threat model No comparison with other protocols Mobility models are not considered Location privacy is not considered
[50]	VANET	User privacy preservation	Attaining conditional privacy preservation on the basis of a lightweight authenticated key establishment scheme	Light weighted authenticated key	Computational overhead Communication overhead Storage overhead -Limited consideration of routing requirements
[51]	VANET	Interest privacy	Resolving the issues of authentication and privacy in VANET such	High privacy	No comparison with other protocols Mobility models are not considered

[32] investigated a beaconing based information distribution and its obstacles have been discussed. This work was first one to identify the problems occurred by the radio shadowing because of stationary and mobile obstacles. A static period beaconing and also abstemiously reactive adaptive could not manage with bigger network dynamics that initiated through shadowing. Our findings provides an innovative challenges like safeguarding fewer transmission dormancy for security applications and extensive variety information distribution for effectiveness requests, then they also deliver prospects because of an integrally condensed station capacity. The signal shadowing negative effects was occurred by adjacent vehicles and the structures that extends beyond the limits. The dynamic beaconing was investigated in this work and a novel algorithm, Thus from the resultant performance it was proved that this approach can destructively speed up beaconing, leads to very low broadcast interruptions, while rapidly reacting to excess circumstances.

[33] elucidated about the localization system in VANETs. In vehicular networks, localization is one of the important critical challenge for providing the extremely correct and dependable localization data. There may be chances of getting rapid changes over network topology with its unique features like flexibility restraints, motorist's performance, and the high-speed movement of vehicles that leads towards the distribution of out-of-date localization information. For evading this issue, the future locations of the vehicles could be predicted and it can be used. Here, the data fusion localization

was used as an extension for predicting localization. In this work, the future prediction of the vehicle position was considered and the time-space window of a vectorial trajectory was used as an advantage in this approach. The localization prediction was studied and analyzed in this work for improving VANET applications. In this approach, the localization approaches were surveyed and board following and period sequence forecast methods was cast-off for estimating forthcoming prediction of vehicles.

5. CONCLUSION

This survey aims at describing several approaches regarding VANET. The standards for wireless access in VANET, security issues, VANET application, and an empirical study on the issue challenges tools and techniques of the VANET service were discussed with its merits and demerits. There were several techniques that were implemented for various application. However, there some limitations on the existing techniques which could be overcome. The brief review handled on techniques can be utilized for future research and it helps the researchers to improve their work.

REFERENCES

1. G. K. Rajbahadur, *et al.*, "A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety," in *2018 IEEE Intelligent Vehicles Symposium (IV),* 2018, pp. 421-426. https://doi.org/10.1109/IVS.2018.8500383
2. A. M. Pushpa and K. Kathiravan, "A comparative survey of security solutions for multicast and unicast routing protocols in mobile ad hoc networks," *International Journal of Wireless and Mobile Computing,* vol. 10, pp. 232-249, 2016. https://doi.org/10.1504/IJWMC.2016.077221
3. N. K. Chaubey, "Security analysis of vehicular ad hoc networks (VANETs): a comprehensive study," *International Journal of Security and Its Applications,* vol. 10, pp. 261-274, 2016. https://doi.org/10.14257/ijsia.2016.10.5.25
4. J. Cheng, *et al.*, "Routing in Internet of Vehicles: A Review," *IEEE Trans. Intelligent Transportation Systems,* vol. 16, pp. 2339-2352, 2015. https://doi.org/10.1109/TITS.2015.2423667
5. M. Mozaffari, *et al.*, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *arXiv preprint arXiv:1803.00680,* 2018.
6. F. Aznoli and N. J. Navimipour, "Deployment strategies in the wireless sensor networks: systematic literature review, classification, and current trends," *Wireless Personal Communications,* vol. 95, pp. 819-846, 2017. https://doi.org/10.1007/s11277-016-3800-0
7. G.-H. Chang, *et al.*, "An Attribute-based Fine-grained Access Control Scheme in Vehicular Ad-hoc Networks," in *Proceedings of the 2017 International Conference on Wireless Communications, Networking and Applications*, 2017, pp. 40-44. https://doi.org/10.1145/3180496.3180604
8. F. A. Silva, *et al.*, "Vehicular networks: A new challenge for content-delivery-based applications," *ACM Computing Surveys (CSUR),* vol. 49, p. 11, 2016. https://doi.org/10.1145/2903745
9. K. A. Hafeez, *et al.*, "Optimizing the control channel interval of the dsrc for vehicular safety applications," *IEEE Transactions on Vehicular Technology,* vol. 65, pp. 3377-3388, 2016. https://doi.org/10.1109/TVT.2015.2440994
10. Y. Yao, *et al.*, "Multi-channel based Sybil Attack Detection in Vehicular Ad Hoc Networks using RSSI," *IEEE Transactions on Mobile Computing,* 2018.
11. A. Mammeri, *et al.*, "Video streaming over vehicular ad hoc networks using erasure coding," *IEEE Systems Journal,* vol. 10, pp. 785-796, 2016. https://doi.org/10.1109/JSYST.2015.2455813
12. A. K. Tyagi and N. Sreenath, "Location privacy preserving techniques for location based services over road networks," in *Communications and Signal Processing (ICCSP), 2015 International Conference on,* 2015, pp. 1319-1326. https://doi.org/10.1109/ICCSP.2015.7322723
13. D. He, *et al.*, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security,* vol. 10, pp. 2681-2691, 2015. https://doi.org/10.1109/TIFS.2015.2473820
14. A. Reyes, *et al.*, "Communication technologies to design vehicle-to-vehicle and vehicle-to-infrastructures applications," *Latin Am. Appl. Res,* vol. 46, pp. 29-35, 2016.
15. A. Oranj, *et al.*, "Routing algorithm for vehicular ad hoc network based on dynamic ant colony optimization," *Int. J. Electron. Elect. Eng,* vol. 4, pp. 79-83, 2016. https://doi.org/10.18178/ijeee.4.1.79-83
16. R. E. Elahi, *et al.*, "Applications of Vehicular Ad-hoc Network (NANET)," 2017.
17. M. Jain and R. Saxena, "Overview of VANET: Requirements and its routing protocols," in *Communication and Signal Processing (ICCSP), 2017 International Conference on*, 2017, pp. 1957-1961. https://doi.org/10.1109/ICCSP.2017.8286742
18. E. C. Eze, *et al.*, "Advances in vehicular ad-hoc networks (VANETs): Challenges and road-map for future development," *International Journal of Automation and Computing,* vol. 13, pp. 1-18, 2016. https://doi.org/10.1007/s11633-015-0913-y
19. H. A. Omar, *et al.*, "Wireless access technologies for vehicular network safety applications," *IEEE Network,* vol. 30, pp. 22-26, 2016. https://doi.org/10.1109/MNET.2016.7513860
20. H. Hasrouny, *et al.*, "VANet security challenges and solutions: A survey," *Vehicular Communications,* vol. 7, pp. 7-20, 2017. https://doi.org/10.1016/j.vehcom.2017.01.002
21. F. Cunha, *et al.*, "Data communication in VANETs: Protocols, applications and challenges," *Ad Hoc Networks,* vol. 44, pp. 90-103, 2016. https://doi.org/10.1016/j.adhoc.2016.02.017

22. Y. Cao, *et al.*, "A scalable and cooperative MAC protocol for control channel access in VANETs," *IEEE Access*, vol. 5, pp. 9682-9690, 2017. https://doi.org/10.1109/ACCESS.2017.2706020
23. C. Sommer, *et al.*, "Simulation tools and techniques for vehicular communications and applications," in *Vehicular ad hoc Networks*, ed: Springer, 2015, pp. 365-392.
24. A. Rasheed, *et al.*, "Vehicular ad hoc network (VANET): A survey, challenges, and applications," in *Vehicular Ad-Hoc Networks for Smart Cities*, ed: Springer, 2017, pp. 39-51.
25. R. Begum, *et al.*, "A Survey on VANETs Applications and Its Challenges," in *International Conference on Advanced Computer Science and Software Engineering (ICACSSE)*, 2016, pp. 1-7.
26. A. K. Ali, *et al.*, "Drop-burst length evaluation of urban VANETs," 2017.
27. M. A. Ferrag, *et al.*, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, pp. 3015-3045, 2017.
28. G. Singh, *et al.*, "A clustering based intrusion detection system for storage area network," *International Journal of Computer Applications*, vol. 88, 2014.
29. W. Viriyasitavat, *et al.*, "Vehicular communications: Survey and challenges of channel and propagation models," *arXiv preprint arXiv:1505.06004*, 2015.
30. X. Hou, *et al.*, "Vehicular fog computing: A viewpoint of vehicles as the infrastructures," *IEEE Transactions on Vehicular Technology*, vol. 65, pp. 3860-3873, 2016. https://doi.org/10.1109/TVT.2016.2532863
31. S. A. A. Shah, *et al.*, "Adaptive beaconing approaches for vehicular ad hoc networks: A survey," *IEEE Systems Journal*, vol. 12, pp. 1263-1277, 2018.
32. C. Sommer, *et al.*, "How shadowing hurts vehicular communications and how dynamic beaconing can help," *IEEE Transactions on Mobile Computing*, vol. 14, pp. 1411-1421, 2015.
33. L. N. Balico, *et al.*, "Localization Prediction in Vehicular Ad Hoc Networks," *IEEE Communications Surveys & Tutorials*, 2018.
34. X. Liang, *et al.*, "Profile matching protocol with anonymity enhancing techniques," in *Security and Privacy in Mobile Social Networks*, ed: Springer, 2013, pp. 19-41. https://doi.org/10.1007/978-1-4614-8857-6_2
35. R. Lu, *et al.*, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE transactions on vehicular technology*, vol. 61, p. 86, 2012.
36. R. Lu, *et al.*, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Transactions on Vehicular Technology*, vol. 59, pp. 2772-2785, 2010.
37. T. W. Chim, *et al.*, "VSPN: VANET-based secure and privacy-preserving navigation," *IEEE Transactions on Computers*, vol. 63, pp. 510-524, 2014.
38. J. Li, *et al.*, "ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, pp. 938-948, 2015.
39. S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Vehicular Communications*, vol. 9, pp. 19-30, 2017. https://doi.org/10.1016/j.vehcom.2017.02.001
40. J. Zhou, *et al.*, "Security and privacy for cloud-based IoT: challenges," *IEEE Communications Magazine*, vol. 55, pp. 26-33, 2017.
41. J. Zhou, *et al.*, "Secure and privacy preserving protocol for cloud-based vehicular DTNs," *IEEE Transactions on Information Forensics and Security*, vol. 10, pp. 1299-1314, 2015.
42. K. Rabieh, *et al.*, "Efficient Privacy-Preserving Chatting Scheme with Degree of Interest Verification for Vehicular Social Networks," in *GLOBECOM*, 2015, pp. 1-6. https://doi.org/10.1109/GLOCOM.2015.7417514
43. I. Ullah, *et al.*, "VBPC: Velocity based pseudonym changing strategy to protect location privacy of vehicles in VANET," in *Communication Technologies (ComTech), 2017 International Conference on*, 2017, pp. 132-137.
44. J. Ni, *et al.*, "Privacy-preserving data forwarding in vanets: A personal-social behavior based approach," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, 2017, pp. 1-6.
45. Z.-C. Liu, *et al.*, "A Realistic Distributed Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks," *IEEE Access*, 2018.
46. T. Gao and X. Deng, "A Pseudonym Ring Building Scheme for Anonymous Authentication in VANETs," in *International Conference on Broadband and Wireless Computing, Communication and Applications*, 2018, pp. 481-489.
47. S. Tanwar, *et al.*, "A systematic review on security issues in vehicular ad hoc network," *Security and Privacy*, vol. 1, p. e39, 2018.
48. R. Yu, *et al.*, "Mixgroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, pp. 93-105, 2016.
49. I. Memon, "A secure and efficient communication scheme with authenticated key establishment protocol for road networks," *Wireless Personal Communications*, vol. 85, pp. 1167-1191, 2015. https://doi.org/10.1007/s11277-015-2833-0
50. B. Libert, *et al.*, "Short group signatures via structure-preserving signatures: Standard model security from simple assumptions," in *Annual Cryptology Conference*, 2015, pp. 296-316.
51. D. Schröder and D. Unruh, "Security of blind signatures revisited," *Journal of Cryptology*, vol. 30, pp. 470-494, 2017. https://doi.org/10.1007/s00145-015-9225-1