Available online at: http://www.ijmtst.com/vol4issue6.html

International Journal for Modern Trends in Science and Technology

ISSN: 2455-3778 :: Volume: 04, Issue No: 06, June 2018

A Review on Misbehaviour Detection And Revocation in VANET

Pranab Garg | Arshdeep Singh | Preeti Shrama

Assistant Professor, Department of CSE, BGIET Sangru, Punjab, India.

To Cite this Article

Pranab Garg, Arshdeep Singh and Preeti Shrama, "A Review on Misbehaviour Detection And Revocation in VANET", *International Journal for Modern Trends in Science and Technology*, Vol. 04, Issue 06, June 2018, pp.-88-95.

DOI: https://doi.org/10.46501/IJMTST040642

ABSTRACT

Vehicular ad hoc networks (VANETs) are emerged technology where vehicles and roadside units(RSUs) communicate with each other. VANETs can be categorized as a sub branch of mobile ad hoc networks(MANETs). VANETs help to enhance traffic efficiency and safety and supply infotainment facility also .Thedissemination of messages must be relayed through nodes in VANETs. However, it's possible that a node maypropagate false information during a network thanks to its malicious behaviour or selfishness. Vehicle unplannedNetwork (VANET) is an emerging and promising technology for the Intelligent transportation (ITS). VANET canhelp to extend safety and traffic efficiency in flexible and feasible way. However, disseminating misinformation inshouldbecatastrophic, results. Misbehaving attackers can create traffic illusion to disturb VANET operations also because thepotential deployment of safety and traffic efficiency applications. during this paper, a holistic view of the prevailingmisbehavior detection approaches for countermeasures against spreading malicious data in VANET is studied.additionally , the importance and therefore the challenges faced when verifying the

Keywords : *Misbehavior detection, Location privacy, Selfish behavior*

I. INTRODUCTION

Vehicular ad hoc network (VANET) consists of vehicles (also mentioned as nodes), road side units (RSUs) andcertification authorities (CAs), whose goal is to make sure road safety and help in secure transfer of messages anddata. Communication can either be vehicle-to- vehicle (V2V) (e.g. relaying alert information) or vehicle-to-infrastructure (V2I) (e.g. when the vehicle must report some event to the RSU/CA). Security in VANETs is vital ,because the message sent by one vehicle may need important consequences like accident prevention.VANETsare acategory of ephemeral networks , where the connection between vehicles (nodes) is brief lived. The topology changes very frequently, as nodes move in and out of range of every other. The density of the networkalso changes over time, e.g. during rush hours. These characteristics make VANET very challengingfor handling security issues.[1] Human behavioral tendencies are going to be reflected within the movement of thevehicles (rational behavior). Vehicles can issue false alerts thanks to either some internal failure and false alerts(faulty nodes), or intentionally for selfish reasons (malicious nodes). Malicious nodes may need criminal motives tocause accidents and should also plan to gather sensitive information about other nodes, e.g. mastercard number fromRFID signals at an electronic toll station. Current research on security in VANETs has been

focused on location privacy, maintaining authenticity of knowledge and revocation of certificates and secretcredentials.Surveys on Thesafety challenges in VANETs are often found. Location privacy is achieved by assigning several pseudonyms (oraliases) to Every vehicle, such two or more pseudonyms belonging to at least one vehicle can't be linked together. Authenticationtechniques believe signatures; a message is signed with a personal key to verify if a user has the corresponding public key. A certificate is additionally issued to verify the validity of the general public key.Signature schemes for VANETs are studied extensively, e.g. ECMV. the problems in revocation problem arewhether to take care of an inventory of all revoked certificates and keys or revoked vehicles or some seed to deduc the list of revoked vehicles. Revocation of certificates andsecret credentials has the subsequent disadvantages. Thecertificate revocation list (CRL) containing all the certificates of revoked vehicles, has got to be sent to all or any thenodes within the network. This approach requires an enormous bandwidth, if the amount of revoked nodes is high.Our approach considers that revocation won't be necessary, because a node which misbehaves once, for selfishreasons, might send correct information at other times. it important, and sometimes necessary, to not disregard theright information. during this paper, we assume that nodes misbehave mostly due to selfish reasons. for instance ,vehicle might send false report on congestion, accident or road block. it conceivable to believe that avehicle doesnt have intentions of causing accidents. Each vehicle normally sends valid and useful information. If allthe certificates are revoked, then useful information sent are going to be ignored. Therefore, we argue thatone don ;t got to classify vehicles consistent with their over all behavior, but instead to differentiate between correctand false information received from the vehicle. it important to spot false data and therefore the sender efficiently,because a delay of even one second might cause an accident. the matter of identifying false data is termed as data-centric misbehavior detection in contrast to entity-centric misbehavior detection, where the most goal is to seekout out andpenalize a knowledge centric misbehavior detection stems misbehaving node. the thought of fromRaya's work on data-centric trust, where the author considers trust on information instead of on the source of data .Once we detect that a node has send false information, this message is shipped to the CA, through the RSUs. The revoke the key credentials (keys/certificates) of the node. Instead, the misbehaving node receives a fine,depending upon its action. It can keep it up sending information which could not necessarily be malicious. Thepayment of fines would hopefully discourage nodes from sending further false messages. We show that ourapproach saves computation and communication bandwidth, which are high thanks to revocation expenses. wemight wish to detect alerts such emergency breaking, approaching emergency vehicles, road feature notifications,change of lanes, etc. Our approach takes under consideration the alert sent by a vehicle and compares it with itsaction taken in response to the alert. is not a legitimate action, then the alert is fake .

II MISBEHAVIOR IN VANETT

Malignant information is the sort of information that is speaks to the ground truth. Getting into mischief hubs maysend bogus data deliberately or because of inadvertent blames in their activities. Trouble making is a term utilized inthe specially appointed systems for any deviation from the normal conduct. In VANET, going astray from typical activity can take numerous structures, for example, sending bogus data, cover some data, mess with messages substance, for example, personality, ready sort, occasion area, hub position, and time, making counterfeit messages,or compelling another hub to send bogus message are viewed as mischievous activities in information and should be recognized each time a message got. A hub is called getting out of hand hub when it can send messages guaranteeing an occasion that either has not happened, or wrong data affirming a genuine occasion, or both, making applications disappointment. For the most part in VANET, mischievous activities can exist at any layer of the network. For instance , in physical layer untouchable aggressors can lunch DoS by sticking assault, mess withequipment, or trick sensors to

send bogus data. In information connect layer vehicles can send sham data by modifying beaconing rate or eating channel catching assault. At organize level, a noxious hub can parody the personality of another hub to get explicit data. Another genuine dangers nearness of dark gap assault on the system where an assailant guarantee its current in best area to advance the data. Wormhole assault where different hubs could be dark opening hubs consented to move the occasion occurred set up to make another occasion in the second spot, for example, mishap. In the application layer vindictive vehicle can create bogus messages, for example,
claiming to be in different areas for example Sybil assault. Sybil assault could be a hotspot for each conceivable assault in VANET It can misdirect some check systems that dependent on the democratic and can execute dark and worm entire assault. Additionally it can send counterfeit data to cause hub fall into counterfeit computational and correspondence overhead. Bad conduct can be purposefully for malignant or egotistical reasons or it very well may be unexpectedly due breakdown of the equipment hardware or other sign related issue, for example, signal misfortune. Figure 1 shows misconduct causes scientific classification. There are two sorts of messages that are utilized for empowering VANET security and traffic proficiency applications. These messages can be grouped dependent on their age: intermittent or occasion driven. Vehicles utilize intermittent messages purported referencepoints for declaring their reality in the system. Reference points are communicated persistently contains position,time and versatility data, for example, speed quickening of the vehicles. Vehicles utilize this data to take moreremote choice about their physical or system practices. For instance in wellbeing application vehicle, vehicle canrecognize strange circum-stances on the streets, for example, mishaps or clogs even before they show up. The secondsort of messages is the occasion driven messages which are come about because of the association among threeitems vehicles, streets, and drivers.

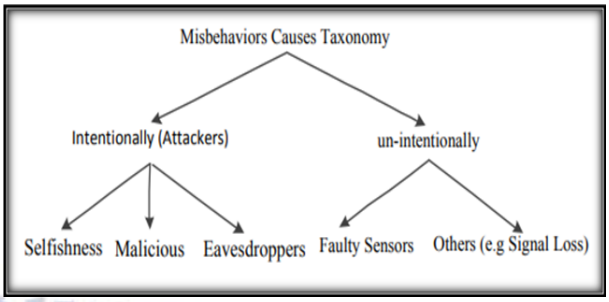

Figure 1: Misbehavior detection causes

111. IMPORTANCE OF MISBEHAVIOR DETECTION IN VANET

For some contemplations, for example, usage cost and accessibility, VANET applications depend on V2V interchanges. Without the foundation, there will be malevolent information. Indeed, even with high security systems, a vehicle can give bogus data accidentally (for example defective hubs) or purposefully by essentially controlling vehicle sensors. Distinguishing malevolent substance is significant for VANET applications. Moreover, most VANET applications will utilize land directing conventions where the position will be utilized to accomplish better steering and upgrade organize execution. Likewise, security and traffic effectiveness needs solid and confided in information. Confirm the believability of VANET information is vital for dependability of the choice taking to evade utilize this data. In addition, recognizing getting into mischief hub that send bogus data is essential to be halted or confined from upset system tasks. As of late, numerous mischief recognition systems have been proposed so as to upgrade VANET security and wellbeing. For responsibility and obligation, distinguishing the making trouble hubs permit specialists to punish the real senderof the bogus data and debilitate the purposefully misbehaving.

IV CHALLENGES

Despite the fact that VANET is viewed as a type of MANET, VANET conduct is on a very basic level unique, even from any current impromptu system. This various presents numerous interesting qualities,for example, fast topology change in light of high portability of the vehicles and causing continuous dis-availability and system division. The availability time length among hubs might be short. Consequently, it is hard to keep up secure and dependable interchanges. System thickness

has high fluctuation in modestquantity of time which prompts versatility or accessibility problems.[As referenced before, VANET isthe source and the objective of the data cause it extremely delicate to messages to contain. For that, bogus messages could be deadly on the applications. For instance, drivers may modify their practices dependent on the information got from dubious condition which could be fetal for individuals life and properties. Afew applications with the end goal that identified with security need severe cutoff time. Anothertestforactualizing VANET applications is client inspirations. Research has indicated that 60% of mishaps could be stayed away from if drivers were cautioned a large portion of a second prior to the effect of a crash.Notwith standing, nearness of pernicious information in the system can prompt corrupt traffic effectiveness or/and cataclysmic mishaps. In the accompanying subsections, we quickly portray a portion of the difficulties of information check in VANET.

Substance Verification

VANE needs forcing solid validation components in which aggressors (for example Sybil) can't mimic different vehicles elements. In any case, in transient system, such VANET, the correspondence between vehicles is short and the topology is quickly changes. For that, versatility, and continuous necessities are significant for secure correspondence in VANET. Confirming information of individual vehicle is imperative to evaluate the conduct of their proprietor. In this manner, connecting numerous messages from single vehicle is required for information check. In the other hand, messages connect capacity is a security concern. Vehicles are close to home property and individuals are very worry about the protection of their data. Drivers won't acknowledge having their development followed by peers. Validation shields vehicles from being mimicked by the Sybil aggressors. In any case, it encourages protection disregarding by permitting assailant connecting the messages of individual vehicle and track their excursion or concentrate their security data, for example, driver name, or vehicle number.

Position Verification

Most VANET application, if not all, relies upon solid position data. At times, vehicle position is utilized as vehicle personality to give secrecy and secure its protection. At that point, in such obscurity situation, Sybil assailants can guarantee its reality in different area, in this way the bogus data can be infused in the system. For instance, an eager driver utilizes various areas to report clog in a particular district of the street causing other vehicle change their courses. Also, vehicle position can be utilized to help directing convention. Besides, situating frameworks, for example, land situating frameworks (GPS) isn't sufficiently exact and it endures accessibility issue for example in the passages, or terrible climate. Additionally, GPS sign can be produced causing vehicles send its reality in bogus positions For the most part, frogged or swindled position can prompt numerous sort of assaults, for example, represented in Figure 2. Sybil assault , dark opening assault , worm gap assault are considered among genuine dangers for VANET security and traffic effectiveness applications

Time Verification

As opposed to the conventional fixed system, VANET may has not get to consistently to focal control. Time is a significant component in VANET for progression of all kind of utilizations message checks. VANETs accept the accessibility of normal wellsprings of time, for example, base-stations or GPS. With the nonattendance of clock synchronization, hubs need contrasting the hour of the up and coming messages with its nearby time. Security applications is time basic wrong time estimation may prompt difficult issue for example mishaps. Vehicles may disregard some significant wellbeing messages while they may be basic because of un-effective time check. What's more, some confirmation procedures needs precise planning among hubs with the end goal that proposed in for position check.

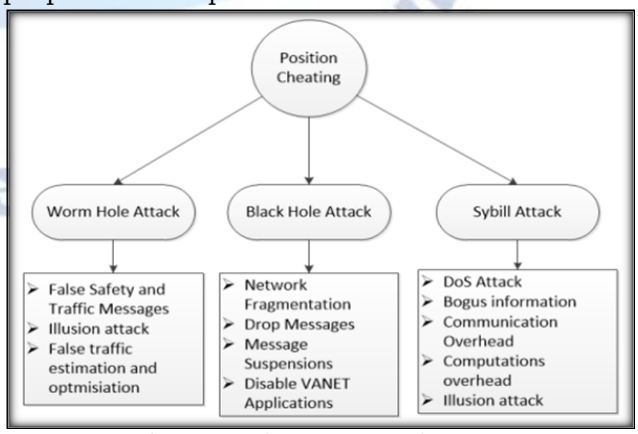

Figure 2 Threats of position cheatin

Versatility Verification

As opposed to data security viewpoint, human factor in VANET forces very test issues. Vehicles development data is an impression of the driving exercises and driver status. Drivers' practices are unpredicted and differed from driver to driver dependent on numerous mental highlights, for example, driver penchant, status, driving time, and numerous other complex highlights. Confirm the rightness or the legitimacy of any detailing circumstance could be outlandish, without relating vehicle conduct to this circumstances and data.moreover, checking the authentic conduct of individual vehicle or driver debilitate the security necessities and increment the recognition delays. Nonetheless, one can profit by the high unique topology change in VANET to fabricate a framework that can follow vehicles practices impermanent on the fly, and afterward, conclude the drivers' practices without disregarding their security. With nearness of numerous dangers, for example, restriction mistakes and flawed vehicles just as the assailants, portability data isn't solid and the choice upon this data might be uncertain.

Occasion Verification

VANET applications have various necessities. For instance, traffic effectiveness applications are postpone tolerant though security applications are time basic. Most security applications hand-off on single expectation correspondences while traffic proficiency applications are multi-jump. Besides, every application has diverse setting. For instance, electronic brake light application needs the deceleration data from vehicles in wellbeing importance region which is inside single expectation inside a region situated before the vehicles while, post-crash warning require a few bounces behind the sender. The credibility of the occasion may not identify with the dependability of the sender that most security procedures mean to give. Vehicles must be certain about the data gotten from open and threatening condition such the case in VANET

DEFENSE AGAINST MISBEHAVIOR IN VANET

Misbehavior detection and data validation is open and active area of research in VANET, especially data related to safety and traffic efficiency. To prevent spreading false information in the network proactive or reactive security mechanisms are used in the literature

Proactive Security Mechanisms

Proactive systems expecting to forestall spreading bogus messages by executing security instruments, for example, Public Key Infrastructure (PKI) or/and computerized signature with or without declaration alongside carefully designed gadgets. For instance, the standard way to deal with give secure correspondence in VANET depends on Entity-Trust, which is stablished by executing open key framework, marking the messages with computerized marks and confirmed through an endorsement gave to vehicle by power. These components triumphs in forestalling outcast assailants and restrict some insider aggressors from spreading deceitful messages. In any case, insider aggressors can produce legitimated bogus data for some reasons deliberately, for example, self-centeredness or vindictive or a flawed vehicle may create bogus messages unexpectedly. Besides, such components confronted numerous difficulties, for example, versatility and complex administration and still open research issues. By and large, cryptographic marks trust foundation doesn't ensure the rightness of the substance particularly when the vehicles have not legitimately associated before with one another's for example multi-jump arrange. Besides, the choice of the accuracy of the data can't be taken by knowing the reliability of the originators. What's more, proactive security systems may endure adaptability issue due its requirement for key administration, denial, and pseudonymous. In any case, it tends to be kept up through a mix of foundation and carefully designed equipment such arrangements found in .

Threshold Based Authentication

Vehicle transfers data just on the off chance that it is valid. One way to deal with embrace messages, a message is valid if it's accounted for by limit number of validated vehicles (accepting dominant part legit) . In any case, this methodology expands the correspondence and calculation overhead. For example, in the clogs numerous vehicles may report the blockage and making system fizzle. Utilizing different marks, for example, connected marks, onion marks, and cross breed marks may not appropriate for time basic applications . As substantiated by Douceur in Sybil assault can make the instruments that utilization repetition flops in disseminated frameworks. In addition, limit based approval is wasteful for security , in light of the fact that wellbeing require fast and precise approval calculations. The need and

challenge in how to utilizing an instrument for approving security on the fly. As indicated by , limit approval instruments consider a subset of the data to approve the messages which may present vindictive data from getting into mischief hub. Utilizing strategies dependent on the substance (Entity-Centric) isn't sufficient to make sure about VANET against bogus data. The supposition that vehicle is mindful or dependable on theirs produced data may preclude vehicles from asserting incorrectly data else they will get correctional activities from the power. Message validation brought exceptionally basic issue up in VANET. Aggressors can connect numerous messages from a vehicle to track or concentrate important data about the drivers . In this manner, protection saving ought to be embraced in the beginning period of security plan. Security can be given through secrecy and unlink capacity for example the message should oppose to be connected together . The stander approach to save protection is to furnish vehicles with nom de plumes. Vehicles utilize distinctive key in each time interim as portrayed in the IEEE standard. As needs be, the aggressor can't connect messages from similar vehicles. Be that as it may, this thusly raised basic security and wellbeing issues. Noxious vehicles can utilize its nom de plume to sign bogus messages and make figment about the traffic. Namelessness urges getting into mischief hubs to send bogus data without fears of the risk. Number of endeavors to adjust security and protection has been proposed in the writing.

Reactive Security Mechanisms

A couple of arrangements have been proposed in the writing plan to supplement proactive countermeasures with receptive methodologies, for example, in . Receptive security systems can be assembled into two classes: Entity Centric recognition approaches and Data believability and consistency draws near. First methodology is called Entity-Centric, which can recognize the making trouble hub. Recognizing getting into mischief hub require a framework have the option to recognize hub elements. Typically, believed foundation dependent on verification with confided in outsider PKI or agreeably for example bunch mark is utilized to give open and private key for every hub. Sender vehicle at that point can utilize computerized mark to sign the message. Beneficiary on the opposite side can distinguish the sender hub by checking its mark. A few instances of Entity-Centric methodologies have been proposed in . The second methodology of location component is Data-Centric in which, the accuracy of the got information is explored as opposed to researching the dependability of the sender. Information credibility and consistency check is utilized to distinguish off base messages. It is like interruption identification frameworks in conventional systems in which vehicles associate the got data with the data definitely known from pervious communication or predefined edges, for example, speed limits. One of the basic issues of bad conduct location in proactive security countermeasures, trouble making discovery instruments could be forceful against anomalous vehicles during some abnormal occasions, for example, mishaps and braking. Along these lines, they will be named making trouble hubs. Another issue identified with information driven rowdiness location, that it urge noxious vehicle to abuse the nonattendance of element check to dispatch Sybil assault. In this way, adjusting security and protection is required with the end goal that in . From opposite side, in information driven security components, protection can be kept up through obscurity be that as it may, it urge vehicles to infuse bogus information unafraid of being followed or rebuffed.

VI EXISTING WORK ANALYSIS

HamssaHasrouny et al. read another structure for the authentication denial process inside VANET. This procedure can be enacted by the Misbehavior Detection Systems (MDSs) running inside vehicles and the Misbehavior Authority (MA) inside the foundation, which distinguishes and bars making trouble vehicles to ensure the long haul usefulness of the system. These MDSs depend on the trust assessment for taking an interest vehicles which is refreshed ceaselessly dependent on their practices. Accordingly, the denial is done occasionally through topographical Certificate Revocation List (CRL) which indicates the testaments of all renounced vehicles inside a particular territory. This outcomes in a lightweight answer for CRL the executives and conveyance inside a secluded and make sure about framework dependent on Public Key Infrastructure (PKI), bunch arrangement and trust assessment. Reenactment situations and hazard investigation were completed indicating the upsides of the proposed renouncement framework.[6] Nandan Parikh et al. proposed Vehicular Ad-hoc Networks (VANETs) are the unique use of Mobile Ad-hoc Networks (MANETs). Because of expanded number of street mishaps, VANETs give wellbeing to street vehicles by a

legitimate coordination with vehicles and street side units. Notwithstanding safety efforts of vehicles, the security of the vehicles has become a significant concern. Vehicles require saving the security of logical data, for example, personality, area, and speed of the vehicle; in any case, with this data a foe can send bogus data to some objective vehicles, which can cause the harm (for example traffic preoccupation, street mishap). Right now, exhibited a protection saving convention for VANET that identifies bad conduct of vehicles. The proposed convention gives start to finish security of vehicles, with the vehicles being mysterious. The convention bolsters information conglomeration by the vehicles, recognizability, and assurance against Sybil assaults, which are significant highlights in present day VANETs.Dinesh Singh et al. broke down the expanded notoriety of web application and savvy urban areas, vehicular specially appointed systems (VANETs) have gotten one of the conspicuous research zone and plentiful of scientists have tended to the numerous issues in the previous decade. Among the numerous issues includes with compelling VANET, bad conduct location and denial is required to address with complete consideration. It is as a matter of first importance step towards managing security applications in VANETs. The vehicle misconduct is answerable for breaking down of many system exercises (e.g., car influx, street mishaps and so on.). The misconduct identification issue turns out to be progressively extreme for wellbeing basic applications in VANETs. The got into mischief vehicle must be renounced from the system as right on time as conceivable to lessen wounds. Along these lines, inconjuction of bad conduct location, repudiation issue likewise should be investigated. This paper is routed to give condition of-workmanship to rowdiness location and denial for security basic VANETs. Here we present a nitty gritty study on important research done in the zone of rowdiness discovery and disavowal with other related issues.

VII CONCLUSION

Misbehavior detection and data verification in VANET are fundamental for executing wellbeing and traffic proficiency applications. Right now, inspected and examined the current methodologies for trouble making discoveries as for various presumptions. The centrality of recognizing noxious information in VANET are depicted with distinguishing the difficulties confronted the execution. At long last, the identification approaches are arranged dependent on their goals into two classes: Entity-Centric or Data Centric methodologies. Every class is talked about and dissected. We are as of now concentrating the misconduct location in more extensive degree. The point is to sum up the recognition components to cover wide scope of VANET applications.

REFERENCES

[1] Drawil, N. M., Amar, H. M., &Basir, O. A. (2012). GPS localization accuracy classification: A context-based approach. IEEE Transactions on Intelligent Transportation Systems, 14(1), pp. 262-273.

[2] El Defrawy, K., &Tsudik, G. (2010). ALARM: Anonymous location-aided routing in suspicious MANETs. IEEE Transactions on Mobile Computing, 10(9), pp. 1345-1358.

[3] Ghafoor, K. Z., Lloret, J., Bakar, K. A., Sadiq, A. S., &Mussa, S. A. B. (2013). Beaconing approaches in vehicular ad hoc networks: A survey. Wireless personal communications, 73(3), pp.885-912.

[4] Ghosh, M., Varghese, A., Gupta, A., Kherani, A. A., &Muthaiah, S. N. (2010). Detecting misbehaviors in VANET with integrated root-cause analysis. Ad Hoc Networks, 8(7),pp. 778-790.

[5] Hartenstein, H., &Laberteaux, L. P. (2008). A tutorial survey on vehicular ad hoc networks. IEEE Communications magazine, 46(6), pp.164-171.

[6] Hasrouny, H., Samhat, A. E., Bassil, C., &Laouiti, A. (2019). Misbehavior detection and efficient revocation within VANET. Journal of Information Security and Applications, 46, pp.193-209.

[7] Hubaux, J. P., Capkun, S., & Luo, J. (2004). The security and privacy of smart vehicles. IEEE Security & Privacy, 2(3), pp. 49-55.

[8] l-Sultan, S., et al. 2014. A Comprehensive Survey on Vehicular Ad Hoc Network. Journal of Network and Computer Applications. 37(0): 380–392.

[9] Lyamin, N., Vinel, A., Jonsson, M., & Loo, J. (2013). Real-time detection of denial-of-service attacks in IEEE 802.11 p vehicular networks. IEEE Communications letters, 18(1),pp. 110-113.

[10] Parikh, N., & Das, M. L. (2017, December). Privacy-preserving services in VANET with misbehavior detection. In 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) , pp. 1-6.

[11] Ruj, S., Cavenaghi, M. A., Huang, Z., Nayak, A., &Stojmenovic, I. (2011, September). On data-centric misbehavior detection in VANETs. In 2011 IEEE Vehicular Technology Conference (VTC Fall) ,pp. 1-5.

[12] Sakiz, F. and S. Sen, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 2017. 61: p. 33-50.

[13] Samara, G., Al-Salihy, W. A., &Sures, R. (2010, May). Security issues and challenges of vehicular ad hoc networks (VANET). In 4th International Conference on New Trends in Information Science and Service Science ,pp. 393-398.

[14] Santamaria, A. F., Sottile, C., De Rango, F., &Voznak, M. (2014, May). Road safety alerting system with radar and GPS cooperation in a VANET environment. In Wireless Sensing, Localization, and Processing IX (Vol. 9103, p. 91030G). International Society for Optics and Photonics.

[15] Singh, D., Ranvijay, & Yadav, R. S. (2018). A state-of-art approach to misbehaviour detection and revocation in VANET: survey. International Journal of Ad Hoc and Ubiquitous Computing, 28(2), pp. 77-93.

[16] Torabi, N., &Ghahfarokhi, B. S. (2017). A bandwidth-efficient and fair CSMA/TDMA based multichannel MAC scheme for V2V communications. Telecommunication Systems, 64(2), pp.367-390.

[17] Van der Heijden, R.W., et al. Enhanced position verification for VANETs using subjective logic. in Proceedings of the 2016 IEEE 84th Vehicular Technology Conference. 2016. Montreal, Canada: Universität Ulm.

[18] Van der Heijden, R.W., et al., Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems. arXiv preprint arXiv:1610.06810, 2016.

[19] Yang, X., Liu, L., Vaidya, N. H., & Zhao, F. (2004, August). A vehicle-to-vehicle communication protocol for cooperative collision warning. In The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004, pp. 114-123.

[20] Zeadally, S., Hunt, R., Chen, Y. S., Irwin, A., & Hassan, A. (2012). Vehicular ad hoc networks (VANETS): status, results, and challenges. Telecommunication Systems, 50(4), pp. 217-241.

[21] Singh, ErSimerpreet, and Narwant Singh Grewal. "Impact of Various Propagation Models on Performance of On-Demand Routing Protocols." (2013).