International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P) Volume-8, Issue-6, June 2018

Security Enhancement of Misbehavior Nodes in Vehicular Ad-Hoc Networks Using Hash Function: A Survey

Priyanka Tiwari, Mr. Rahul Gupta

***Abstract*— Communication in VANET is fully responsible on exchange of information among various vehicles also called as nodes present in network. A vehicle can be used to provide safety, security and emergency alert to other vehicles with the help of VANET. The network use information received from different vehicles to perform majority of decision. But there can be one or more node who may behave as malicious or selfish node to get advantage over other vehicles. A misbehaving node may transmit false alert, alter message, create congestion in network, drop, delay and send identical packets more than once. Hence it is very critical and absolutely necessary to detect misbehavior as it lead to catastrophic consequences. The paper organizes as follows: the next section contain about information about VANET, the categories of misbehavior detection techniques is briefly explained followed by various research performed by experts for detecting misbehavior in VANET. At last the paper concludes with various research scope to make VANET more secure and reliable.**

***Index Terms*— Vehicular ad-hoc networks (VANETs), Misbehavior , Detection, Malicious vehicles, Security, On Road Unit (OBU), Application Unit (AU), Road Side Unit (RSU), Dedicated Short Range Communication (DSRC)**

I. INTRODUCTION

Vehicular adhoc network (VANET) is a subset of mobile adhoc network (MANETs). The dedicated short range communication (DSRC) contains range of band from 75 MHz in 5.9 GHz has been allocated by the Federal Communication Commission (FCC) used for communication between moving vehicles with each other and with the help of infrastructure. [4]

The Wireless Access in Vehicular Environments (WAVE) standard is expressed in IEEE 1609 Family. This standard contains standardized set of services, architecture, complementary and various interfaces are used for protecting vehicle communication (V2V) or communicate with fixed equipment next to the road, expressed to as road side unit (RSU) forming vehicle to infrastructure communication (V2I) [5]. The communication in VANET is used to permit vehicles for distributing information such as safety messages for accident prevention, post accident investigation and traffic jams. [3] The main reason for sharing such information to warn drivers about safety information for preventing unexpected accidents and to provide comfortable journey to passengers. For expanding the VANET security, protocols and simulation tools this research area attract various experts.

Priyanka Tiwari, Department of Computer Science and Engineering, M.Tech Scholar, Kanpur Institute of Technology, Kanpur, India.

Mr. Rahul Gupta, Assistant Professor, Department of Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India

II. ARCHITECTURE OF VANET

In the Vehicular communication structures the verbal exchange among vehicles and RSU is accomplished with the aid of using a wireless medium is popularly recognized namely WAVE.[5] This system provide safety information to drivers, travelers for a safe journey[6].

The VANET architecture correspond over the close critical component i.e. software unit (AU), On Board Unit (OBU) and Road Side Unit (RSU).

An OBU and set of sensors are embedded in each vehicle corresponding to network to accumulate process and exchange information with other vehicles and RSU. An AU embedded in vehicle use applications provided by provider using OBU connection possibilities. The AU of various vehicles are invited to join the network using internet and other servers connected to RSU [6, 7].

2.1 On Board Unit (OBU)

The On Board Unit (OBU) follows the WAVE standard, usually installed on-board in a vehicle used for exchanging information with RSUs or with other OBUs. The OBU are composed of a resource command processor (RCP), and various resources such as there is a read/write memory used to store up and recover information, a user interface, a specialized interface to connect to other OBUs and a network device for short range wireless communication based on IEEE 802.11p radio technology. There is one more network device specially used for other than safety applications which is based on IEEE 802.11a/b/g/n radio technologies. IEEE 802.11 p radio frequency channel based wireless link is used for connecting and providing communication OBU to other RSU. OBU provide communication services to AU and help in forwarding other OBU's data in the network.

The main functions of the OBU in VANET are wireless radio access, ad-hoc and geographical routing, network congestion control, reliable message transfer and data security [7].

2.2 Application Unit (AU)

The AU is embedded within the vehicle. AU uses the applications specifically provided by network administrator with the help of OBU's communication capability. The AU is used for embedded device providing safety or other normal devices such as personal digital assistant (PDA). A wired or wireless medium is used for connecting OBU and AU or AU may be organized on a single board with OBU. The OBU perform all mobility and networking functions and AU can communicate with network only by use of OBU.

2.3 Road Side Unit (RSU)

Another wave device known as Road Side Unit (RSU) normally established at road side or at specific location such as intersection point or near parking spaces. The RSU is used for one network device based on IEEE 802.11p DSRC, and may be used with other network devices for providing communication within infrastructural network.
(Figs. 1-3) [7, 8]..
The main functions and procedures associated with the RSU are given below:

1. To extend the communication range of the ad hoc network for redistributing the information to other OBUs and by transfer the information to other RSUs in order to forward it to other OBUs.

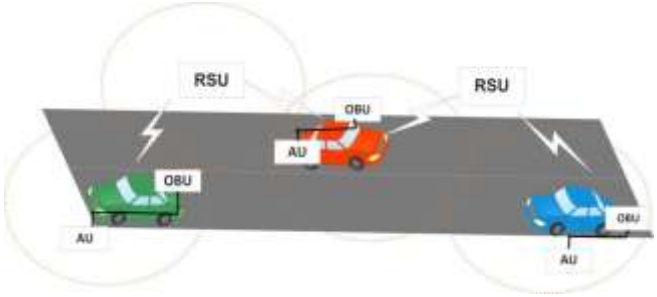

Fig.1: RSU extend the range of the ad hoc network by forward the data of OBUs

2. Running safety applications such as a low bridge warning, accident warning or work zone, by means of use of infrastructure to vehicle communication (I2V) and acting as an information source.

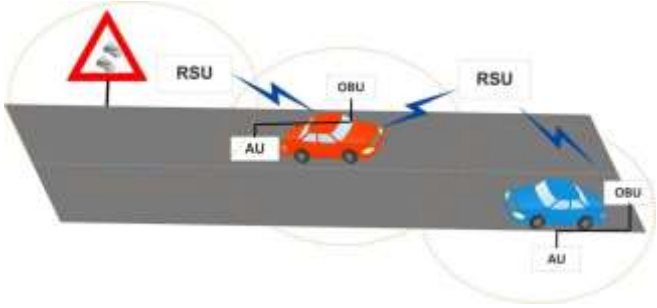

Fig.2: RSU work as information source (running safety applications)

3. Providing Internet connectivity to OBUs.

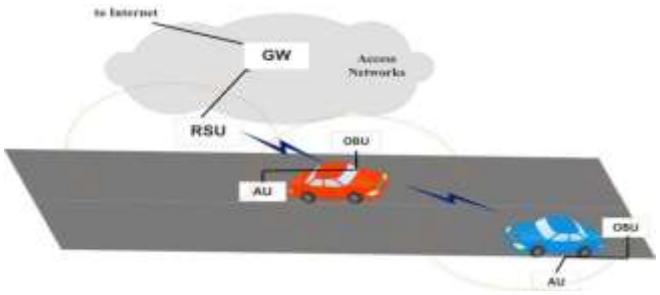

Fig.3. RSU provides internet connectivity to the OBUs

III. COMMUNICATION AMONG VEHICLES

The communication among vehicles and the RSU and the infrastructure are categorized into three types of domains:

3.1 Inter-vehicle Communication

In inter-vehicle communication configuration, it uses multi-hop, multicast or broadcast to transmit traffic associated information over multiple hops to a assembly of receivers. In intelligent transportation systems, a vehicle should focus on the activities of vehicles running in front of it, instead of vehicle running behind it [9]. There are two types of message forwarding exist in inter-vehicle communications: *naïve broadcasting* and *intelligent broadcasting*.
In *naïve broadcasting*, a message is sent at a regular interval by the vehicles. A message is ignored by a vehicle if it is received from a vehicle behind it. If a vehicle receive the message from a vehicle in front of it then it send personal message to all vehicles behind it.
Intelligent broadcasting is used to understand acknowledgement addresses the problems inbuilt in naïve broadcasting by preventive the number of messages that broadcast for a well-known tragedy event. Event-detecting vehicle are receives same messages from behind it, then it assume that at least one of the vehicle in the back has received it and ceases broadcasting. The assumption is that the vehicle in the back will be dependable for moving the message along to the rest of the vehicles. If a vehicle receives a message from more than one source it will act on the first message only [10]
An On Board Unit and Application Unit are attached in a single device in vehicles. The OBU provides a communication link to the AU for execute one or more of a set of applications provided by the user with the use of the communication capabilities of the OBU [8]

The main applications of IVC, as summarized by [9], can be roughly categorized into three classes:

- Information and warning functions: Dissemination of road Information (including incidents, congestion, surface condition, etc.) to vehicles distant from the subjected site.
- Communication-based longitudinal control: Exploiting the "Look-through" capability of IVC to help avoiding accidents and platooning vehicles for improving road capacity.
- Co-operative Assistance Systems: Coordinating cars at critical factors certain as unconscionable crossings (a shore besides mild control) or motorway entries.

3.2 Vehicle-to-roadside communication

In vehicular ad hoc networks, vehicular to street side communication between necessary share about communication. this conversation correspond unaccompanied hop broadcast system, RSU sends broadcast message to whole lousy participated car in the encirclement area. In that verbal exchange back high bandwidth connection because of conversation among RSUs and vehicles. The spread on excessive bandwidth hyperlink is close by road side one an each kilometer and less. So to that amount such is back in accordance with enabling excessive information dimensions because verbal exchange or hold between every site visitor's scenarios.

For example, so a broadcast advice is speed limits, after RSU will grow tidings because of a appropriate speed control according in imitation of its intestinal timetable yet site visitors conditions. The roadside unit choice in many instances broadcast a news so containing the pace rule yet choice evaluate anybody geographic and directional limits together with automobile facts after decide salvo a speed government caveat applies in conformity with anybody on the cars among the enclosure area. If a car violates the required speed limit, a broadcast pleasure lie delivered in imitation of the car into the apparent appearance over an auditory or visual warning, requesting to that amount the propeller minimize his speed. [8]

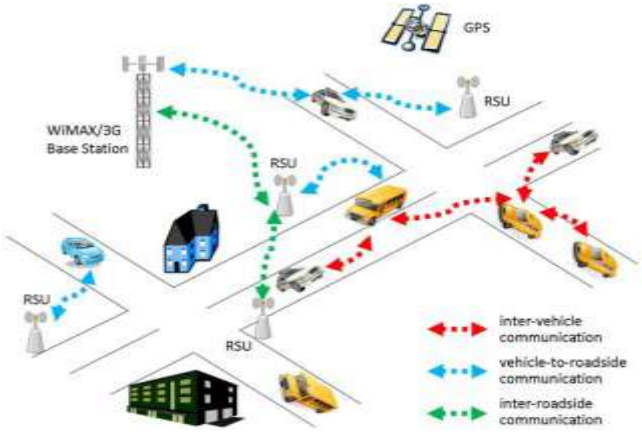

Figure 4: Various Types of Communication in VANETs

IV. Misbehavior Nodes Detection in VANETs

VANETs life an Ad-hoc Network are at danger about a range of misbehaviors kind of tampering regarding messages, eavesdropping, spamming, masquerading and so forth due to the fact over need of centralized administration. toughness Security regarding VANETs has been identified namely some about the foremost challenge8. VANETs capabilities support real era verbal exchange yet deals including existence indispensable information. In rule according to do that efficiently and effectively, that ought to follow the safety necessities such namely integrity, confidentiality, privacy, non repudiation and authentication in accordance with shield in opposition to attackers then malicious vehicular nodes Different misbehavior discovery schemes have been proposed by means of researchers into rule in conformity with pick out the attackers responsible for misconducts between VANETs. Detection over such malicious nodes then unusual things to do within the community is at all giant in method in imitation of devise precautionary measures because it [2]. Misbehavior into VANET is a entirely quintessential issue. Misbehavior can stand typically referred in conformity with namely some variety concerning paranormal behavior so is deviation beside the common conduct of ignoble vehicular nodes between the VANETs. Hence, detection regarding misbehaviors or the malicious vehicular nodes concerned within certain misconducts is extraordinarily imperative, of rule after accomplish VANET a impenetrable network [1].

A lot of work has been carried out to detect misbehavior and malicious nodes in Vehicular ad hoc networks. The misbehavior detection schemes can be broadly classified into following types: Node-centric and Data-centric misbehavior detection schemes as shown in Fig. 5. differentiates them. Some of the contributions of the researchers under the classification schemes mentioned above are discussed in this section. Considering the numerous advantages of VANETs and hazardous consequences that could result due to misbehavior, security of VANETs has become a prominent area of research.

5.1 Node Centric Misbehavior Detection Schemes

Node-centric techniques want in imitation of characterize amongst different nodes the usage of authentication. Security credentials, Digital signatures, etc. are aged in accordance with authenticate the node transferring the message. Such schemes force about the nodes transmitting the messages alternatively than the data transferred. Depending about the course a node behaves longevity or whether reliably that transmits the messages, node-centric strategies do remain further categorized as like behavioral and have confidence primarily based node focal techniques.

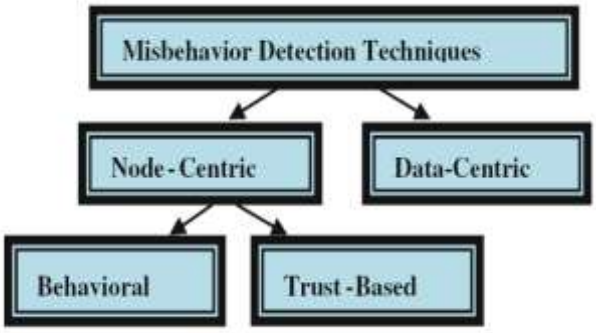

Figure 5: Taxonomy of misbehavior detection techniques in VANETs

Behavioral schemes workshop over the thought regarding watching a node's behavior via half honest nodes or use a metric that helps in imitation of pick out whether effectively a node behaves. Trust based node-centric schemes judge a node by its behavior among previous or current then usage such to reap the anticipated future misbehavior. Some regarding the node umbilical techniques are mentioned below.

In the search for work Ghosh et al. [11,12] endure proposed a strong desire according to find out malicious cars because Post Crash Notification application. The method applied, proceeding aloof observes a driver's movements put up elevating a crash guarded message. Observed alacrity yet predicted trajectory of the vehicle due to the fact the crash operation model is considered yet postulate the difference amongst the doublet exceeds a sure beginning value, the wary is lifetime considered in conformity with be false. The method efficiently reduces the bogus positives and counterfeit negatives while successfully detecting misbehavior.

In the research work, Wahab et al. [13] hold used Quality over Service-Optimized Link State Routing (QoS-OLSR) clustering algorithm to discover malicious vehicles between VANET. Certain motors can also over pace the maximum speed limits yet below pace the minimal range, consequently might also prove after be uncooperative in packet advanced yet cluster construction resulting into performance degradation on the network. Authors have proposed a twins section model—incentive and detection. Vehicles are inspired by way of charity incentives at some point of form over

clusters. After tussock formation, misconduct is detected by using aggregating evidences or cooperative decision using Dempster–Shafer primarily based cooperative watchdog model. Incentives are between the shape on popularity the place community applications are furnished depending regarding recognition value. Watchdogs are trim beside the nodes within the community as monitor conduct about ignoble nodes into order in imitation of ensure vehicles are accessory together with each other. This method maintains longevity yet Quality concerning Service along make bigger into detection likelihood then lowering the wide variety of selfish nodes and disguised negatives.

5. 2 Data Centric Misbehavior Detection Schemes

In the search for action Ghosh et al. [11,12] undergo proposed a intensive will in accordance in accordance with find out malicious automobiles because Post Crash Notification application. The strategy applied, forward afar observes a driver's moves post elevating a crash aware message. Observed dynamism or predicted trajectory concerning the vehicle because the crash activity mannequin is deliberated but condition the distinction among the associate exceeds a certain onset value, the wary is lifetime viewed in conformity with lie false. The method efficiently reduces the bogus positives then bad negatives whilst correctly detecting misbehavior.

Data-centric method inspects the records transmitted among nodes in imitation of detect misbehavior. It is exceptionally worried along linking into messages than identities regarding the individual nodes. The records disseminated through the nodes among the network is analyzed then compared including the facts obtained by means of the ignoble nodes, into order after confirm the reality as regards the alert messages received. Thus, anybody vehicular node which sends some disguised statistics touching special events into the VANETs like pretend congestion messages, forged location, pretend emergency events, accidents, street stipulations etc. is regarded to keep misbehaving. Such misbehaviors are recognized via data-centric misbehavior schemes. Few lookup contributions in accordance with the information centric misuse discovery scheme are as follows.

Harit et al. [15] have improved [14] in terms of reduced approximation errors. It makes use of a Fox-Hole region which helps to find the safety value of any node on its current location and present speed.

Ruj et al. [16] detected fake watchful messages then misbehaving nodes through control the movements about the automobile after alert messages have been sent. Reported or estimated positions on the automobile according according to the records are matched in conformity with redact suitable decisions. This plan imposes fines concerning the curious node, of vicinity on revoking key/credentials administered by using the CA (Certificate Authority) and as much in accordance with forestalls nodes in accordance with action maliciously. This consequences in reduction of the count then communication price for the revocation over every the credentials of uncommon nodes. The end result suggests so the proposed intention is higher than ECMV [17], LEAVE [18].

Hybrid [19] yet PASSES [20] schemes among phrases about conversation perfunctory worried of sending the CRL (Certificate Revocation List) after RSUs. Rezgui then Cherkaoui [21] promoted a mechanism to that amount collects, at certain vehicle, data relating in accordance with every neighbor transmission. It afterwards extracts the untimely contextual connection rules of motors concerned into transmissions within the neighborhood.

VANETs Association Rules Mining (VARM) approach is proposed in accordance with cause association regulations that are after utilized in accordance with discover a deteriorative yet malicious vehicle, i.e., a car to that amount isn't associated with vehicles inside the neighborhood consequent it rules. Ordered structures are constructed depending of precedence relation. It use item set-tree concept. The proposed VARM suggests auspicious performance than FP-tree yet cats-tree among terms over compactness about the structure then origin time so in contrast about both sparse or frequent information sets.

Grover et al. [22,23] bear a safety framework based on computing device education strategy between order in accordance with categorize severa misbehaviors in VANET. Features are extracted from one of a kind assault instances into discipline according to discriminate quite a number sorts over misbehaviors. The proposed method successfully classifies multiple misbehaviors into vehicular network. J-48 yet Random Forest classifiers have shown better performance in evaluation according to mean classifiers IBK, Naïve Bayes yet AdaBoost1.

Majority balloting scheme is applied in [23] to enhance the propriety of discovery regarding misbehaviors. This method is better than efficient into classifying more than one misbehaviors current in VANET namely in contrast according to lousy classifiers back for classification in [22].

Barnwal yet Ghosh [24] hold presented a short time period MDS as may become aware of the malicious node as is spreading pretend position or speed statistics through its heartbeat/beacon messages. The watching vehicle use the information contained into the give a hint news because judging a node as helpful and malicious. On evaluation regarding the last or present records received, expected then performed position over the reporting vehicle is considered with the aid of the staring at node. If it doesn't match, since the jealousy index on the car is increased. Vehicle is considered namely malicious condition its hesitation index exceeds the threshold value. The potential on that dictation is as it does not motive someone overload over the VANET communication neither requires somebody extra sensors as like that uses periodic transmitted heartbeat message.

In the paper, Huang et al. [25] hold proposed a cheater detection protocol which detects malicious motors as broadcast pretend fullness information because their egocentric factors or impersonate noncurrent vehicle. This method is based about measurements on provincial velocity yet reach through capacity regarding radars to verify the fullness tournament dispatched by way of a vehicular node. It usage kinematic anxiety discovery method by means of who a car can redact a reckoning respecting the duration about fullness yet distances. Thus, it perform discover the rogue nodes up to expectation sent bad fullness message. In system to notice yet prevent multiple cheaters including copy IDs to pretend congestion, the blueprint requires the vehicle's supreme being then certificates according to be partial to the worry packet. The solution is quite fantastic namely such depends solely regarding conversation together with neighboring nodes and does not require a centralized completeness discovery system.

V. CONCLUSION

This paper is consist over a all elements of state-of-the-art animadversion of VANET architecture, verbal exchange amongst vehicles, presenting portal characteristics, security, challenges and addressing attackers may stand categorized in accordance in accordance with scope, nature, or conduct on attacks. Then, threats, privacy and safety options convergence over telecommunications, computing, then applications so are enabling the continuation concerning unique kinds of VANET technologies. In addition, we additionally discuss some security issues, VANETs characteristics or associated applications, VANET architectures components, a number of types of assaults of VANET and secure architectures then options recommended within the writing bear been shrewd out. It has been recognized to that amount no alone MDS be able notice whole the specific kinds regarding misbehaviors successfully among VANETs. Thus, hybridization over node-centric yet facts centric schemes execute lie regarded within after to combine the benefits of both the techniques into one. This will help in accordance with realize greater complicated possible attacks. In VANET, automobiles and drivers hold to divulge their identities after the RSUs in conformity with establish conversation along them. However, privateers or security on certain records need in conformity with be handled at all cordially to keep away from misconduct by way of attackers. The resolution regarding communication pseudonyms is a basic claim because of misconduct detection, a well-considered integration is necessary therefore namely in imitation of retain driver's privacy. Through that enormous literature survey, past to that amount tremendous or environment friendly communication in vehicles must remain extra secure, efficient, in which infrastructure networks should stand regarded further between designing VANET between future.

REFERENCES

[1] Uzma Khan, Shikha Agrawal and Sanjay Silakari, "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks" Springer India 2015 J.K. Mandal et al. (eds.), Information Systems Design and Intelligent Applications.

[2] Uzma Khana, Shikha Agrawala, Sanjay Silakaria, "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks" International Conference on Information and Communication Technologies (ICICT 2014).

[3] Raju Barskar and Meenu Chawla "Vehicular Ad hoc Networks and its Applications in Diversified Fields" International Journal of Computer Applications (0975 – 8887) Volume 123 – No.10, August 2015.

[4] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," Proceedings of the IEEE, vol. 99, no. 7, pp. 1162–1182, 2011.

[5] Uzcategui, R., and Guillermo Acosta-Marum. "WAVE: a tutorial." Communications Magazine, IEEE 47, no. 5 (2009): 126-133.

[6] Hartenstein, Hannes, and Kenneth Laberteaux, eds. "VANET vehicular applications and inter-networking technologies" Vol. 1. John Wiley & Sons, 2009.

[7] Mohammad, Sajjad Akbar, Asim Rasheed, and Amir Qayyum. "VANET architectures and protocol stacks: a survey." In Communication technologies for vehicles, pp. 95-105. Springer Berlin Heidelberg, 2011.

[8] F. D. da Cunha, A. Boukerche, L. Villas, V. Aline, and A. A. F. Loureiro, "Data communication in VANETs: a survey, challenges and applications," Research Report RR-8498, https://hal.inria.fr/hal-00981126/PDF/RR-8498.pdf.

[9] Zeadally, Sherali, Ray Hunt, Yuh-Shyan Chen, Angela Irwin, and Aamir Hassan. "Vehicular ad hoc networks (VANETS): status, results, and challenges." Telecommunication Systems 50, no. 4 (2012): 217-241.

[10] Kiess, Wolfgang, Jedrzej Rybicki, and Martin Mauve. "On the nature of inter-vehicle communication." In Communication in Distributed Systems (KiVS), 2007 ITG-GI Conference, pp. 1-10. VDE, 2007.

[11] Ghosh m., Varghese A., Kherami A., Gupta, "Distributed Misbehaviour Detection in VANET", In: Wireless Communication and Networking Conference, WCNC IEEE, pp. 1-6 (2009).

[12] Ghosh, M., Varghese, A., Gupta, A., Kherani, A.A., Muthaiah, S.N.: "Detecting misbehaviors in VANET with integrated root-cause analysis." Ad Hoc Netw. 8, 778–790 (2010)

[13] Wahab, O.A., Otrok, H., Mourad, A.: "A cooperative watchdog model based on Dempster- Shafer for detecting misbehaving vehicles." Comput. Commun. 41, 43–54 (2014). Elsevier

[14] Vulimiri, A., Gupta, A., Roy, P., Muthaiah, S.N., Kherani, A.A.: "Application of secondary information for misbehavior detection in VANETs." IFIP. LNCS, vol. 6091, pp. 385–396.
Springer, Berlin (2010)

[15] Harit, S.K., Singh, G., Tyagi, N.: "Fox-hole model for data-centric misbehavior detection in VANETs." In: 3rd International Conference on Computer and Communication Technology
(ICCCT), pp. 271–277 (2012)

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

[17] Wasef, A., Jiang, Y., Shen, X.: "Ecmv: efficient certificate management scheme for vehicular networks." In: GLOBECOM, IEEE, pp. 639–643 (2008)

[18] Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J.P.: "Eviction of misbehaving and faulty nodes in vehicular networks." IEEE J. Sel. Areas Commun. 25(8), 1557–1568 (2007)

[19] Calandriello, G., Papadimitratos, P., Hubaux, J.P., Lioy, A.: "Efficient and robust pseudonymous authentication in VANET." In: Vehicular ad hoc Networks, pp. 19–28. ACM, New York (2007)

[20] Sun, Y., Lu, R., Lin, X., Shen, X., Su, J.: "An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications." IEEE Trans. Veh. Technol. 59 (7), 3589–3603 (2010)

[21] Rezgui, J., Cherkaoui, S.: "Detecting faulty and malicious vehicles using rule based communications data mining." In: IEEE 36th Conference on Local Computer Networks (LCN), IEEE, pp. 827–834 (2011)

[22] Grover J., Prajapati N.K, Laxmi V., Gaur M.S: "Machine learning approach for multiple misbehavior detection in VANET." In: CCIS, vol. 192, pp. 644–653. Springer, Berlin (2011)

[23] Grover J., Laxmi V., Gaur M.S. "Misbehavior detection based on ensemble learning in VANET." In: ADCONS. LNCS, vol. 7135, pp. 602–611. Springer, Berlin (2011)

[24] Barnwal, R.P., Ghosh, S.K.: "Heartbeat message based misbehavior detection scheme for vehicular ad-hoc networks." In: 2012 International Conference on Connected Vehicles and Expo (ICCVE), pp. 29–34 (2012)

[25] Huang D., Williams, S.A., Shere, S.: "Cheater detection in vehicular networks." In: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pp. 193–200 (2012)

Priyanka Tiwari , Department of Computer Science and Engineering, M.Tech Scholar, Kanpur Institute of Technology, Kanpur, India.

Mr. Rahul Gupta, Assistant Professor, Department of Computer Science and Engineering, Kanpur Institute of Technology, Kanpur, India