

A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks

Uzma Khan, Shikha Agrawal and Sanjay Silakari

Abstract Communication in Vehicular ad hoc Network relies on exchange of information among different vehicular nodes in the network. This helps to improve the safety, driving efficiency and comfort on the journey for the travellers. In this network, information received from other vehicles is utilized to make majority of the decisions. However, a node may behave malicious or selfish in order to get advantage over other vehicles. A misbehaving node may transmit false alerts, tamper messages, create congestion in the network, drop, delay and duplicate packets. Thus, detecting misbehavior in VANET is very crucial and indispensable as it might have disastrous consequences. This paper presents a detailed survey on some of the important research works proposed on detecting misbehavior and malicious nodes in VANETs. In addition to the details about the techniques used for misbehavior detection, nature of misbehavior, this paper categorizes the schemes for better understanding and also outlines several research scopes to make VANET more reliable and secure.

Keywords Vehicular ad-hoc networks (VANETs) • Misbehavior • Detection • Malicious vehicles • Security

U. Khan (✉) • S. Agrawal • S. Silakari

Department of Computer Science and Engineering, University Institute of Technology,
RGPV, Bhopal, India

e-mail: uzma.khans@gmail.com

S. Agrawal

e-mail: shikha@rgtu.net

S. Silakari

e-mail: ssilakari@yahoo.com

© Springer India 2015

J.K. Mandal et al. (eds.), *Information Systems Design and Intelligent Applications*,
Advances in Intelligent Systems and Computing 339,
DOI 10.1007/978-81-322-2250-7_2

1 Introduction

Nowadays, Vehicular ad hoc Network has gained much attention to incorporate security on transportation systems. Vehicular ad hoc Network is an ad hoc Network which is considered as a subclass of Mobile ad hoc Network (MANET). VANET exhibits numerous special features such as high mobility, rapidly changing network topology, frequent partitioning etc. As a result of these unique characteristics, many solutions and protocols proposed for MANET might not be suitable or directly applicable to VANETs. Thus VANET needs for its unique solutions [1].

Security of VANETs has been identified as one of the major challenge. VANETs applications support real time communication and deals with life critical information. In order to do it correctly and effectively, it must follow the security requirements such as integrity, confidentiality, privacy, non repudiation and authentication to protect against attackers and malicious vehicular nodes. There are several attacks like black hole, Sybil, DoS, Timing, Illusion etc. which not only affect the driver's and vehicle's privacy but also compromise traffic safety and may lead to loss of life [2]. Thus, in order to become a real technology that assures traffic safety VANETs require appropriate security techniques and mechanisms that will guarantee protection against various misbehaviors and malicious nodes that affects security of VANET. Figure 1 shows the VANET architecture.

In Sect. 1, we have given a brief introduction about VANETs. Section 2 discusses the importance of malicious node detection and classification of misbehavior node detection techniques in VANETs. We present various efforts by researchers under

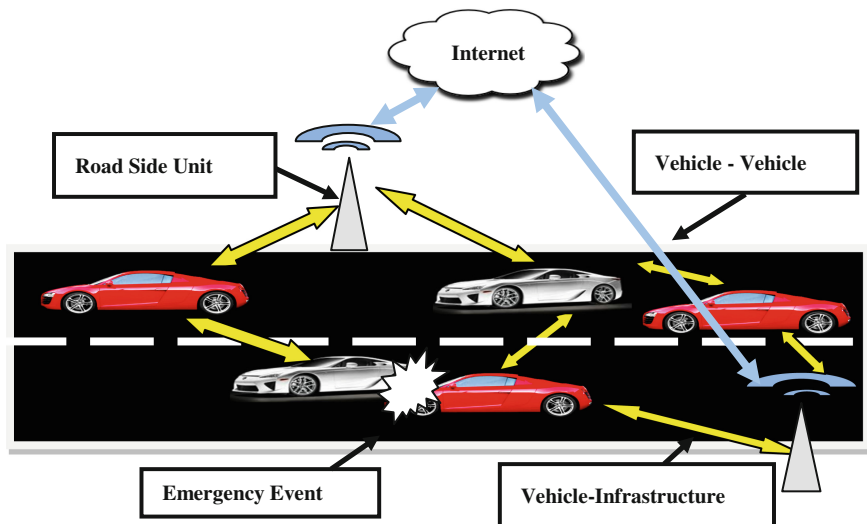


Fig. 1 Vehicular ad hoc network architecture

Node-Centric and Data-Centric Misbehavior Detection Techniques in Sects. 3 and 4 respectively. Section 5 concludes the review work with discussion and some future research ideas.

2 Misbehavior Nodes Detection in VANETs

Information dissemination in VANETs happens through cooperative behaviour of the vehicular nodes. Messages transmitted in vehicular network carry vital information like traffic jam, emergency brake events, road conditions, accident notifications, bad weather conditions, etc. In such a case, if any vehicle act maliciously and tamper with the messages, the results may be very dangerous. Thus misbehaviors in VANET is a very crucial issue. Misbehavior can be generally referred to as any kind of abnormal behaviour that is deviation from the average behaviour of other vehicular nodes in the VANETs. Hence, detection of misbehaviors and the malicious vehicular nodes involved in such misconducts is extremely imperative, in order to make VANET a secure network. 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. 2. Table 1 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.

3 Node Centric Misbehavior Detection Schemes

Node-centric techniques need to distinguish among different nodes using authentication. Security credentials, Digital signatures, etc. are used to authenticate the node transferring the message. Such schemes emphasis on the nodes transmitting the messages rather than the data transferred. Depending on the way a node behaves

Fig. 2 Taxonomy of misbehavior detection techniques in VANETs

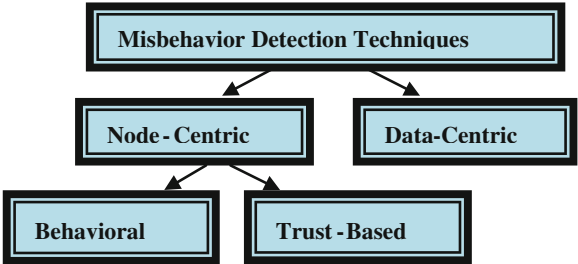


Table 1 Node-centric versus data-centric misbehavior detection techniques

	Based on	Simplicity	Attackers	Additional requirements	Number of misbehavior detected	Overhead
Node centric detection	Authentication of nodes, behavioral and trust analysis	Techniques employed to isolate malicious nodes are simpler	Able to detect insider attackers	Require enhanced OBU's, sensors and radars for monitoring	Limited	Less
Data centric detection	Analyzing the data transmitted among nodes	Complex algorithms and comparisons are used to detect discrepancy in data	Able to detect misbehaviors caused by insiders as well as outsider attackers	Need fast computation capable devices for quick data processing	Many	More

and how reliably it transmits the messages, node-centric techniques can be further categorized as behavioural and trust based node-centric techniques. Behavioural schemes works on the concept of observing a node's behaviour by some trustworthy nodes and uses a metric that helps to identify how effectively a node behaves. Trust based node-centric schemes judge a node by its behaviour in past and present and uses it to obtain the expected future misbehavior. Some of the node centric techniques are discussed below.

In the research work Ghosh et al. [3, 4] have proposed a robust scheme to detect malicious vehicles for Post Crash Notification application. The approach applied, firstly observes a driver's actions post raising a crash alert message. Observed mobility and expected trajectory of the vehicle for the crash mobility model is calculated and if the difference between the two exceeds a certain threshold value, the alert is considered to be false. The approach effectively reduces the false positives and false negatives while effectively detecting misbehavior. In [8] Ghosh et al. improved their previous work [7] by considering the possibility of the fake position information of the vehicle in the PCN along with the false crash alert. The cause-tree representation is used effectively to conjointly accomplish misbehavior detection in addition to identification of its root-cause by employing logical reduction. The scheme proves to be robust and achieves considerable detection of misbehavior.

Kim and Bae [5] have proposed a novel misbehavior based reputation management scheme (MBRMS) which includes three components (a) Misbehavior detection (b) Event rebroadcast and (c) Global eviction algorithms for the detection and filtration of false information in VANETs. Each vehicular node maintains information system of events and corresponding actions for the detection of misbehaving node. The presented mechanism uses outlier detection technique and misbehaving risk value of the bad node to measure the risk level. MBRMS effectively detects and evicts the misbehaving nodes.

In the research work, Daeinabi and Rahbar [6] have proposed the Detection of Malicious Vehicles (DMV) algorithm through observation to discover malicious nodes that drop or duplicate received packets more than a given threshold value. Vehicles are tagged using a distrust value and are monitored by the allocated verifier nodes. Black and white lists are maintained in order to isolate the malicious vehicles from the honest vehicles. It has been observed in simulation that detection of malicious vehicles is faster in case of Constant Speed Motion (CSM) and Smooth Motion Model (SMM) as compared to Fluid Traffic Model (FTM). Performance analysis shows that this misbehavior detection scheme is capable of finding out most existence malicious vehicles even at quite high speeds. Kadam and Limkar [7] have presented an improvement of the DMV algorithm [6]. It not solely detects malicious nodes however additionally their prevention from the VANET. This approach reduced the impact of black hole attack within the VANET and is more efficient and secure compared to DMV.

In the research work, Wahab et al. [8] have used Quality of Service-Optimized Link State Routing (QoS-OLSR) clustering algorithm to detect malicious vehicles in VANET. Certain vehicles may over speed the maximum speed limits or under speed the minimum range, thus may prove to be uncooperative in packet forward

and cluster formation resulting in performance degradation of the network. Authors have proposed a two phase model—incentive and detection. Vehicles are motivated by giving incentives during formation of clusters. After cluster formation, misbehavior is detected by aggregating evidences and cooperative decision using Dempster–Shafer based cooperative watchdog model. Incentives are in the form of reputation where network services are provided depending on reputation value. Watchdogs are appointed from the nodes in the network that monitor behaviour of other nodes in order to ensure vehicles are cooperating with each other. This method maintains stability and Quality of Service with increase in detection probability and decreasing the number of selfish nodes and false negatives.

4 Data Centric Misbehavior Detection Schemes

Data-centric approach inspects the data transmitted among nodes to detect misbehavior. It is primarily concerned with linking between messages than identities of the individual nodes. The information disseminated by the nodes in the network is analyzed and compared with the information received by the other nodes, in order to verify the truth about the alert messages received. Thus, any vehicular node which sends some bogus information about different events in the VANETs like fake congestion messages, false location, fake emergency events, accidents, road conditions etc. is considered to be misbehaving. Such misbehaviors are identified through data-centric misbehavior schemes. Few research contributions to the data centric misbehavior detection scheme are as follows.

Vulimiri et al. [9] have proposed a probabilistic misbehaviour detection approach, based on the secondary information or alerts that are created in response to the primary alerts for PCN application. Secondary alerts are thus used to verify the truth and falsity of the primary alerts received by a vehicle. The secondary information received in the form of other causal alerts can be collated to produce a degree of trust for the primary messages. The observed behaviour is compared with the alert sent by the vehicle to verify the conditions for raising the alert. Hence, if the two don't justify one another, it indicates that the alert is fake and hence the vehicle is malicious. Harit et al. [10] have improved [9] 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. [11] detected fake alert messages and misbehaving nodes by monitoring the actions of the vehicle after alert messages have been sent. Reported and estimated positions of the vehicle according to the information are matched to make suitable decisions. This scheme imposes fines on the misbehaving node, in place of revoking key/credentials administered by the CA (Certificate Authority) so as to prevent nodes to act maliciously. This results in reduction of the computation and communication cost for the revocation of all the credentials of misbehaving nodes. The result shows that the proposed scheme is better than ECMV [12], LEAVE [13],

Hybrid [14] and PASS [15] schemes in terms of communication overhead involved in sending the CRL (Certificate Revocation List) to RSUs.

Rezgui and Cherkaoui [16] developed a mechanism that collects, at one vehicle, information relating to every neighbour transmission. It then extracts the temporal correlation rules between vehicles concerned in transmissions within the neighbourhood. VANETs Association Rules Mining (VARM) method is proposed to generate association rules which are then utilized to find a faulty or malicious vehicle, i.e., a vehicle that isn't related with vehicles within the neighbourhood following these rules. Ordered structures are constructed depending on precedence relation. It uses itemset-tree concept. The proposed VARM shows superior performance than FP-tree and cats-tree in terms of compactness of the structure and execution time when compared on both sparse and dense data sets.

Grover et al. [17, 18] have presented a security framework based on machine learning approach in order to categorize numerous misbehaviors in VANET. Features are extracted from different attack cases in order to differentiate various types of misbehaviors. The proposed approach efficiently classifies multiple misbehaviors in vehicular network. J-48 and Random Forest classifiers have shown better performance in comparison to other classifiers IBK, Naïve Bayes and AdaBoost1. Majority voting scheme is applied in [18] to improve the accuracy of detection of misbehaviors. This approach is better and efficient in classifying multiple misbehaviors existing in VANET as compared to base classifiers used for classification in [17].

Barnwal and Ghosh [19] have presented a short term MDS which can detect the malicious node that is spreading fake position and speed information through its heartbeat/beacon messages. The observing vehicle uses the information contained in the beacon message for judging a node as honest or malicious. On analysis of the last and present information received, expected and observed position of the reporting vehicle is calculated by the observing node. If it doesn't match, then the suspicion index of the vehicle is increased. Vehicle is considered as malicious if its suspicion index exceeds the threshold value. The advantage of this system is that it does not cause any overload on the VANET communication neither requires any additional sensors as it utilizes periodic transmitted heartbeat message.

In the paper, Huang et al. [20] have proposed a cheater detection protocol which detects malicious vehicles that broadcast fake congestion information for their selfish motives and impersonate non existing vehicle. This approach is based on measurements of local velocity and distance by means of radars to verify the congestion event sent by a vehicular node. It uses kinematic wave detection approach by which a vehicle can make a prediction about the duration of congestion and distance. Thus, it can detect the rogue nodes that sent bogus congestion message. In order to detect and prevent multiple cheaters with forge IDs to fake congestion, the scheme requires the vehicle's signature and certificate to be attached to the wave packet. The presented solution is quite effective as it depends only on communication with neighbouring nodes and does not require a centralized congestion detection system.

5 Discussion and Future Work

VANETs have gained a lot of attention as it can greatly improve the safety on roads and driving conditions. Detecting misbehaviors in VANETs is very significant as it can be hazardous. This survey work aims to provide a detailed overview of the various misbehavior detection schemes in VANETs. It is expected that this survey can serve as a helpful guide for the researchers inquisitive about misbehavior detection schemes in VANET and mitigates further research in order to make VANET more secure. Various misbehavior detection techniques have been categorized as Node-Centric and Data Centric Misbehavior Detection Techniques. However, these techniques have certain issues which need to be removed to make VANET more reliable and safe.

The node-centric schemes can be further improved by selecting nodes as observer or verifier after proper authentication. These schemes require good observations and processing the vehicle's actions well to identify the abnormal behaviour, thus there is a need of high speed computation and processing hardware over the OBU to make decisions speedily and accurately. Few misbehavior detection schemes consider the results of the short term misbehavior, however it should be analyzed along with the long term examination for much reliable and better decision making. In Data-centric approach, the detection carried out using the beacon, safety alert messages etc. reduces the extra overhead involved in using sensors and communication of additional messages. But, if the truth parameter value of the information received is not computed speedily, the message may become useless. Hence, efficient processing devices must be equipped in vehicles. Also, inappropriate conclusions drawn from information gathered or overlooking important details could result in poor detection and other misleading decisions. Efficient learning techniques can be used to extract accurate correlation of the events and relationship between vehicular nodes to identify misconducts.

It has been identified that no single MDS can detect all the different types of misbehaviors effectively in VANETs. Thus, hybridization of node-centric and data-centric schemes can be considered in future to integrate the advantages of both the approaches into one. This will help to detect more complicated possible attacks. In VANET, vehicles and drivers have to disclose their identities to the RSUs to establish communication with them. However, privacy and security of such information need to be handled very carefully to avoid misuse by attackers. The resolution of communication pseudonyms is a basic demand for misconduct detection, a well-considered integration is important so as to preserve driver's privacy.

References

1. Wang, Z., Chigan, C.: Countermeasure uncooperative behaviors with dynamic trust-token in VANETs. In: IEEE International Conference on Communications, ICC'07, pp. 3959–3964 (2007)
2. Al-kahtani, M.S.: Survey on security attacks in vehicular ad hoc networks (VANETs). In: 6th IEEE International Conference on Signal Processing and Communication Systems (ICSPCS), pp. 1–9 (2012)
3. Ghosh, M., Varghese, A., Kherani, A.A., Gupta, A.: Distributed misbehavior detection in VANETs. In: Wireless Communications and Networking Conference, WCNC IEEE, pp. 1–6 (2009)
4. 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)
5. Kim, C.H., Bae, I.H.: A misbehavior based reputation management system for VANETS. *LNEE* **181**, 441–450 (2012)
6. Daeinabi, A., Rahbar, A.G.: Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks. *Multimedia Tools Appl.* **66**(2), 325–338 (2013)
7. Kadam, M., Limkar, S.: D and PMV: new approach for detection and prevention of misbehave/malicious vehicles from VANET. In: Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2013. AISC, vol. 247, pp. 287–295. Springer, Heidelberg (2014)
8. Wahab, O.A., Otok, H., Mourad, A.: A cooperative watchdog model based on Dempster-Shafer for detecting misbehaving vehicles. *Comput. Commun.* **41**, 43–54 (2014). Elsevier
9. 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)
10. 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)
11. 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)
12. Wasef, A., Jiang, Y., Shen, X.: Ecmv: efficient certificate management scheme for vehicular networks. In: GLOBECOM, IEEE, pp. 639–643 (2008)
13. 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)
14. 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)
15. 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)
16. 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)
17. 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)
18. 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)
19. 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)
20. 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)

Information Systems Design and Intelligent Applications
Proceedings of Second International Conference INDIA
2015, Volume 1

Mandal, J.K.; Satapathy, S.C.; Kumar Sanyal, M.; Sarkar,
P.P.; Mukhopadhyay, A. (Eds.)

2015, XXX, 889 p. 325 illus., Softcover

ISBN: 978-81-322-2249-1