Misbehavior Node Detection in Vehicular ad-hoc Networks: A survey, With Special Emphasis on Multihop Broadcast Protocols

Zahra Soltani Mohammadi [1], Kiarash Mizanian [1], Mehdi Agha Sarram [1], Salman Goli [2]

[1.] Department of Computer Engineering, Yazd University, Yazd, Iran
[2.] Department of Computer Engineering, Kashan University, Kashan, Iran
soltani.z@stu.yazd.ac.ir

Abstract: VANETs are a subset of Mobile Ad-hoc Networks (MANETs) in which communication nodes are mainly vehicles. Communication in Vehicular ad hoc Network relies on cooperation between vehicles but, 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 that we emphasis on misbehavior detection in multi hop broadcast protocols because of their importance in information dissemination in VANETs. This paper outlines several research scopes to make VANET more reliable and secure.
[Soltani Mohammadi Z, Mizanian K, Sarram MA, Goli S. **Misbehavior Node Detection in Vehicular ad-hoc Networks: A survey, With Special Emphasis on Multihop Broadcast Protocols.** *Researcher* 2017;9(1):41-46]. ISSN 1553-9865 (print); ISSN 2163-8950 (online). http://www.sciencepub.net/researcher. 7. doi:10.7537/marsrsj090117.07.

Keywords: Vehicular ad-hoc Networks; Misbehavior Node detection; Multi Hop Broadcast; Security

1. Introduction

In recent years, vehicular ad hoc network (VANET), have attracted attention of many researchers in the field of mobile and wireless communications, for their application in improving the safety of roads and passenger comfort. VANET is based on short-range wireless communication between vehicle-to-vehicle and some roadside infrastructure. Moreover, a large number of Certification Authorities (CAs) will exist, where each CA is responsible for the identity management of all vehicles registered in its region (e.g., national territory, district, country) (Wang and Chigan, 2007).

Several types of messages are exchanged among vehicles such as traffic information, emergency incident notifications and road conditions. It is important to forward correctly messages in VANET, however, attacker nodes may damage the messages. Attackers or malicious vehicles perform in several ways and have different objectives, such as attackers eavesdrop the communication between vehicles, drop, and change or inject packets into the network. Therefore, one solution is that vehicles should cooperate together to enhance the security performance of a network. Therefore, security mechanisms, facilities and protocols are needed to diminish and to eliminate the attacker's effect.

Although VANET is a specialized form of well known Mobile Ad hoc Networks (MANETs), it exhibits many special features, such as it's extremely high dynamics and mobility, the rapidly changing network topology, limited temporal and functional network redundancy, frequent fragmentation/ partitioning, etc. All these features lead to new challenges during VANET deployment. As a result, many existing MANET solutions would not be suitable for VANET, and VANET requires its unique security solutions.

Along considering all advantages of VANET, this network have many challenges. For example to determine whether the sender of the message, is a legitimate node and receiver node can relay that message immediately, is a big challenge. Otherwise the vehicle may be faced with delay, wrong information, going to unknown routes, pay a fine or even accident. So misbehavior detection, as soon as possible and in the early stage that the road traffic is controllable, is vital and necessary) Jain and Mathuria, 2013).

The remainder of the paper is organized as follows. In section 2, we give a brief outline of misbehavior problems in VANET. In Section 3, we review the related works that is done for detection techniques and in section 4, we'll specially focus on misbehavior detection in VANET broadcast protocols. Finally, we'll present our conclusions in Section 5.

2. Misbehavior Problems In VANET

Vehicular ad-hoc Networks (VANETs) applications are based upon the cooperative behavior of the vehicular nodes and information dissemination through them. 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.

Out of several security concerns, the misbehaving vehicles inside the network, are the major threats to the VANET and participating nodes. The unknown/unauthenticated attacker can be detected and filtered out with the help of IEEE 1609.2 standards (IEEE Std, 2006) based Public Key Infrastructure (PKI) security mechanism. However, the main problem arises when an authenticated node does not behave properly in the network. This type of node is known as a misbehaving node. Nodes misbehave either unintentionally, due to malfunctioning of its sensing equipment or intentionally, for taking illegal benefits or creating trouble in the peer-to-peer network. Irrespective of the reasons, misbehaving nodes pose a big threat to VANET. Moreover, it is unsafe for the communicating vehicles to blindly rely on the received messages that are originating from such misbehaving nodes.

Based upon the motives, the misbehaviors in VANET can be broadly classified into two classes (Khan and Mauri, 2014):

- Intentional misbehavior

This class of misbehavior results from the wrong intention of networked nodes to get the unnecessary benefits by not cooperating with their peers. Some examples of intentional misbehavior in VANET, for instance, are raising bogus alert messages, dropping/delaying of routing packets, un-cooperative behavior during collective decision making, denial for message relay, spoofing of identity, dissemination of false information to the peers, and so on.

- Unintentional misbehavior

This class of misbehavior is normally due to reasons that are not in control of the participating users and purely unintentional. The users of misbehavior nodes of this class are usually not aware of his undesired behavior pattern. For instance, generating wrong alert messages due to a faulty OBU, false positional information due to malfunction of onboard sensors, and malicious behaviors by the compromised nodes are some examples of unintentional misbehavior in VANET.

3. Misbehavior Detection in VANET

Considering the numerous advantages of vehicular ad hoc networks and also dangerous consequences of misbehaviors nodes, the security between vehicles requires special attention and recognizing misbehavior vehicle, is inevitable. Many researches have been conducted to detect misbehavior node in VANET and we classify them in two category as shown in Fig 1. In Continue, we'll describe the methods are mentioned above and we'll survey the last work has done in that classes.

3-1. Node centric misbehavior detection

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

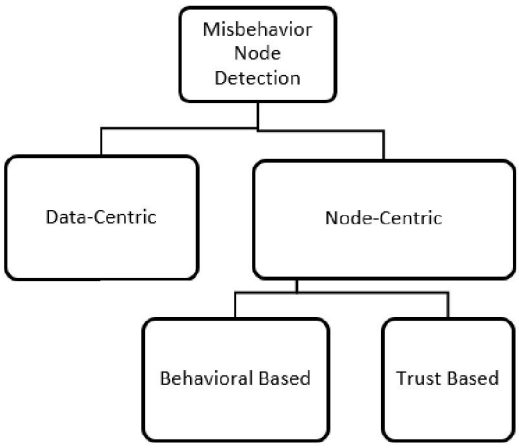

Fig. 1 Taxonomy of Misbehavior Detection

Ghosh et al. (2009) have proposed and analyzed the performance of a Misbehavior Detection Scheme (MDS) for Post Crash Notification (PCN) application. The proposed approach relies on observing the driver's behavior after receiving an alert. Based on other neighborhood or visual inputs, the driver can determine if there is really a crash or if the alert is false. This initial work assumes that even in a false alert, the position information will be correct, which may not be true in practice. They investigated the design of a MDS that does not require this assumption, hence allowing for a broader and more practical misbehavior model. Ghosh et al. (2010) illustrated the basic cause-tree approach and used it effectively to jointly achieve misbehavior detection as well as identification of its root-cause.

Biswas et al. (2010) introduced a new scheme for safety message authentication in VANETs. In their proposed scheme, a road side controller (RSC) is responsible for controlling all the RSUs, and delivering messages through RSUs to vehicles in a given area, where each RSU uses a proxy signature mechanism based on Elliptic Curve Cryptography (ECC), which is a variation of known ECDS-based proxy signature schemes and modified according to the VANET's criteria and security requirements. The underlying network constraints and properties from VANET standards have been taken into consideration along with the security, reliability and other related issues. In our scheme, an adversary can't forge an RSU, or a compromised RSU can't broadcast false, altered, and expired safety message. The approach has low communication overhead, which is compliant to the IEEE802.11p/WAVE standards as it uses the basic ECDSA signature scheme for the proxy signature in RSUs.

Daeinabi et al. (2013) proposed the Detection of Malicious Vehicles (DMV) algorithm through monitoring to detect malicious nodes that drop or duplicate received packets and to isolate them from honest vehicles, where each vehicle is monitored by some of it trustier neighbors called verifier nodes. If a verifier vehicle observes an abnormal behavior from vehicle V, it increases distrust value of vehicle V. The ID of vehicle V is then reported to its relevant Certificate Authority (CA) as a malicious node when its distrust value is higher than a threshold value. Performance evaluation shows that DMV can detect most existence abnormal and malicious vehicles even at high speeds.

Kadam and Limkar (2013) presented new approach for not only the detection of malicious vehicles attack but also their prevention from the VANET. Proposed algorithm is referred as Detection and Prevention of Malicious Vehicles (D&PMV). The malicious vehicles detected using the monitoring process over the VANET, once they are detected, proposed algorithm is applied for the prevention of the same. The detection of malicious vehicles is based on DMV algorithm presented earlier.

A watchdog (Hortelano et al., 2010) is the basic component for the construction of most of the intrusion detection systems proposed so far for self-organizing wireless networking systems like VANETs. The main idea behind watchdog is that, because a node can listen to the packets traversing its neighborhood, it can monitor their activity. Therefore, watchdogs act in promiscuous mode, thus overhearing all next nodes forwarding transmissions. With the information about the neighborhood behavior, the watchdog can deduce if nodes are acting as selfish, black or greyhole routers. According to researches have done by (Soomro, Hasbullah, 2010; Raw, Singh, 2013; van et al., 2013; Makwana et al., 2013; Hernández-Orallo et al., 2015; Naveen Kumar, 2016) can be seen that the Watchdog is used as the core component of many intrusion detection system mechanisms.

Wahab et al. (2014) addressed the problem of detecting misbehaving vehicles in Vehicular Ad Hoc Network (VANET) using Quality of Service Optimized Link State Routing (QoS-OLSR) protocol (Wahab et al., 2013). According to this protocol, vehicles might misbehave either during the clusters' formation by claiming bogus information or after clusters are formed. A vehicle is considered as selfish or misbehaving once it over-speeds the maximum speed limit or under-speeds the minimum speed limit, where such a behavior will lead to a disconnected network. They proposed a two-phase model that is able to motivate nodes to behave cooperatively during clusters' formation and detect misbehaving nodes after clusters are formed. Incentives are given in the form of reputation and linked to network's services to motivate vehicles to behave cooperatively during the first phase. Misbehaving vehicles can still benefit from network's services by behaving normally during the clusters' formation and misbehave after clusters are formed. To detect misbehaving vehicles, cooperative watchdog model based on Dempster–Shafer is modeled where evidences are aggregated and cooperative decision is made. Simulation results show that the proposed detection model is able to increase the probability of detection, decrease the false negatives, and reduce the percentage of selfish nodes in the vehicular network, while maintaining the Quality of Service and stability.

Rupareliya et al. (2016) identified attacker using watchdog and apply Bayesian filter to avoid/reduce false positive of node, recognized by watchdog. In their schema Watchdog method is used to detect the malicious node but what if the node is actually not a malicious node. So to detect that they used Bayesian filter to check whether the detected node is actually a malicious node or not.

Wahab et al. (2016) addressed the problem of detecting malicious vehicles in clustered VANETs. A cluster based cooperative detection model, called CEAP, is advocated. In CEAP, the cluster members are designated as watchdogs to monitor and collect evidences on the behavior of the Multi-point relay (MPR) nodes that are responsible for forwarding the packets on behalf of the cluster. Thereafter, the SVM learning technique is employed to classify MPRs either cooperative or malicious. The proposed detection model reduces the training set size of the SVM classifier, this model is able to operate in highly mobile environment and increase the accuracy of

detections, enhance the attack detection rate, decrease the false positive rate, and improve the packet delivery ratio in the presence of high mobility compared to the classical SVM-based, Dempster Shafer-based, and averaging-based detection techniques.

Yao-Hua Ho et al. (2016) proposed an OMD to support location-based routing protocols for VANET. In OMD scheme, number of LD packet (LD_Count), forwarding request packets (FR_Count), and forwarded packet (F_Count) are used to calculate node's RS (Reputation Score). Nodes detect each other for any misbehavior based on the RS. They extended two location-based routing protocols (i.e. CBF and CLA) with OMD. Various experiments are conducted to study the effectiveness of OMD scheme. The simulation results showed that the proposed technique is able to effectively identify any misbehavior nodes with slightest false accusation (i.e. About 2 – 3 nodes) under different settings.

3-2. Data centric misbehavior detection

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 (Khan et al., 2015). Few research contributions to the data centric misbehavior detection scheme are as follows.

Vulimiri et al. (2010) investigated the use of correlated information, called "secondary alerts", generated in response to another alert, called as the "primary alert" to verify the truth or falsity of the primary alert received by a vehicle. We first propose a framework to model how such correlated secondary information observed from more than one source can be integrated to generate a "degree of belief" for the primary alert.

Rezgui et al. (2011) proposed a rule-based data mining fault detection technique to detect faulty/malicious vehicles in VANETs based on exchanged routine messages. A side advantage of VARM scheme is that correlated information, displayed via association rules, are easy to understand and subsequently easy to log by humans.

Machine learning algorithms have been applied in this issue, Grover et al. (2011) presented a machine learning approach to classify multiple misbehaviors in VANET using concrete and behavioral features of each node that sends safety packets. A security framework is designed to differentiate a malicious node from legitimate node. They implement various types of misbehaviors in VANET by tampering information present in the propagated packet. These misbehaviors are classified based upon multifarious features like speed-deviation of node, received signal strength (RSS), number of packets delivered, dropped packets etc. Experiment result showed that Random Forest and J-48 classifiers perform better compared to other classifiers.

Grover et al. (2011) presented an ensemble based machine learning approach to classify misbehaviors in VANET. The performance of classifiers used for classification depends on the induction algorithms. They exploit the strengths of different classifiers using an ensemble method that combines the results of individual classifiers into one final result in order to achieve higher detection accuracy.

Huang et al. (2012) focused on congestion cheaters in vehicular networks who report non-existing high-way congestion information. They have developed a cheater detection protocol, in which each vehicle only depends on local velocity and distance measurements to validate the congestion event sent by a vehicle. Their presented protocol is based on the traffic flow theory to detect the Kinematic wave caused by congestion. The presented cheater detection solution is effective in that it only requires vehicles to communicate with their neighboring vehicles without relying on a centralized controlled congestion detection and prediction system.

Razzaqu et al. (2014) presented a misbehavior detection scheme (MDS) and corresponding framework based on the mobility patterns analysis of the vehicles in the vicinity of concerned vehicles. Initial simulation results demonstrate the potential of the proposed MDS and framework in message's correctness detection, hence its corresponding applications in collision avoidance.

Kumar et al. (2016) proposed a Historical Feedback based Misbehavior Detection Algorithm (HFMDA) to detect the misbehavior vehicles inside from the network. In this algorithm, an observer vehicle sends a notification to the nearest RSU against a crash-event occurred on the road. Here we assume that all vehicles accumulate its past history for event notifications. All the vehicles maintains this history with two parameters: Event Notifications (EN) and True Event Notification (TEN). In proposed HFMD algorithm, a vehicle's historical record is firstly check to know its past misbehavior history and an RSU_Verification algorithm is used to verify the status of current received notification at the RSU. The proposed hybrid algorithm i.e. data centric and event

centric, is a RSU side algorithm instead of vehicle side.

4. Misbehavior detection in VANET multi hop broadcasting

As is mentioned before, the main objective of vehicle to vehicle communication is improving the road and drivers safety, through exchange of alert messages between cars. Many applications, for notifying other vehicles and road information, traffic congestion, proximity of other vehicles, accidents, delivery notifications and even information related to entertainment programs need multi hop broadcast protocol (Korkmaz et al., 2004; Palazzi et al., 2007; Ravi et al., 2007; Rohini et al., 2015). As a result according to the alert message's nature and safety application that should be delivered in early stages, it is concluded that the multi-hop broadcasting is the most efficient way for message dissemination in VANET. A lot of multi hop broadcast algorithms have proposed so far and, in a few of them, like (Jaballah et al., 2014) security issue and misbehavior detection have been considered. In that research, jaballah et al. considered position cheating, non-cooperation and Refusing to publish a warning, as misbehavior and evaluated them in the IVC-based safety applications and for that they considered a state-of-the-art protocol that is representative of this class of applications: the fast multi hop broadcast algorithm (FMBA) (Palazzi et al., 2007) Also Rohini et al. (2015) have stated that there is a few work in multi hop dissemination protocols for VANETs.

5. Conclusions and future works

Nowadays VANET has attracted a lot of attention because of it's role in improving the road and driver's safety. However, there are many issues that must be addressed before deployment of the VANET in a real scenario. Misbehavior detection in VANET is one such issue. Due to the dangerous effect of misbehavior nodes in this network and the difficulty of it's detection, many researches have done in this topic. Although multi hope dissemination have important role in VANET but There is no fool proof security solution available for detection and isolation of misbehaving nodes in this type of protocols. In this paper we surveyed different types of misbehaviors and their detection techniques in vehicular ad-hoc networks in two category: data centered and node centered and as we mentioned there are a few works for overcome to the misbehavior especially in multi hop protocols. The effort has been made to provide the current state of research in this field. Several recent proposals have been discussed briefly to present a glimpse of several possibilities and approaches suggested by researchers worldwide. A hybrid approach for designing better MDS is proposed for eliminating the limitations of independent and cooperative MDSs. In the future, it is important to focus on the adoption of hybrid approaches for detection of misbehaving nodes in multi hop dissemination protocols in vehicular networks. For future work, the combination of machine learning techniques to detect misbehavior to obtain better result in performance and accuracy, is proposed. Also using fuzzy logic decision making technique in relay node selection with considering it's misbehavior probability is another direction for future works.

Corresponding Author:
Zahra Soltani Mohammadi
Department of Computer Engineering
Yazd University
Yazd, Iran
E-mail: soltani.z@stu.yazd.ac.ir

References

1. Biswas S and Mišić J., Establishing trust on VANET safety messages, in International Conference on Ad Hoc Networks, pp. 314-327, 2010.
2. Daeinabi A. and Rahbar A. G., Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks, Multimedia tools and applications, vol. 66, pp. 325-338, 2013.
3. Ghosh M, Varghese A, Kherani A, and Gupta A., Distributed misbehavior detection in VANETs, in 2009 IEEE Wireless Communications and Networking Conference, pp. 1-6, 2009.
4. Ghosh M, Varghese A, Gupta A, Kherani A., and Muthaiah S. N., Detecting misbehaviors in VANET with integrated root-cause analysis, Ad Hoc Networks, vol. 8, pp. 778-790, 2010.
5. Grover J., Prajapati N. K., Laxmi V., and Gaur M. S., Machine learning approach for multiple misbehavior detection in VANET, in International Conference on Advances in Computing and Communications, pp. 644-653, 2011.
6. Grover J., Laxmi V., and Gaur M. S., Misbehavior detection based on ensemble learning in vanet, in International Conference on Advanced Computing, Networking and Security, pp. 602-611, 2011.
7. Huang D., Williams S. A., and Shere S., Cheater detection in vehicular networks, in 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, pp. 193-200, 2012.
8. Ho Y.-H., Lin C.-H., and Chen L.-J., On-demand Misbehavior Detection for Vehicular Ad Hoc Network, International Journal of Distributed Sensor Networks, vol. 12, p. 155, 2016.
9. Hortelano J, Ruiz J. C., and Manzoni P., Evaluating the usefulness of watchdogs for intrusion detection

in vanets, in 2010 IEEE International Conference on Communications Workshops, pp. 1-5, 2010.
10. Hernández-Orallo M. O. E., Cano J. C., Calafate C. T., Manzoni P., CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes, IEEE Transactions on Mobile Computing, vol. 14, pp. 1162 - 1175, 2015.
11. IEEE Std 1609.2-2006, IEEE trial-use standard for wireless access in vehicular environments—Security services for applications and management messages, 2006.
12. Jain S, Mathuria A, and Das M.L., Security, Privacy, Trust, and Resource Management in Mobile and Wireless Communications, pp.134, IGI Global, 2013.
13. Khan S, Mauri J. L., Security for Multihop wireless Networks, Crc Press, 2014.
14. Kadam M. and Limkar S., D&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), pp. 293-303, 2014.
15. Kumar A., Singh J. R., Singh D., and Dewang R. K., A Historical Feedback Based Misbehavior Detection (HFMD) Algorithm in VANET, in Computational Intelligence and Networks (CINE), 2016 2nd International Conference on, pp. 15-22, 2016.
16. Korkmaz G., Ekici E., Özgüner F., and Özgüner Ü., Urban multi-hop broadcast protocol for inter-vehicle communication systems, in Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 76-85, 2004.
17. Makwana N. P., Vithalani S. K., and Dhanesha J. D., Intrusion Detection-Watchdog: For Secure AODV Routing Protocol in VANET, International Journal of Engineering Trends and Technology (IJETT), vol. 4I, p. 2151, 2013.
18. Naveen Kumar A. P. K. S. K., Detecting Misbehaving and Selfish Nodes in the Network using Watchdog Mechanism, International Journal of Advanced Engineering, Management and Science (IJAEMS), vol. 2, p. 404, 2016.
19. Palazzi C. E., Ferretti S., M. Roccetti, Pau G., and Gerla M., How do you quickly choreograph inter-vehicular communications? A fast vehicle-to-vehicle multi-hop broadcast algorithm, explained, 2007.
20. Ravi N., Smaldone S., Iftode L., and Gerla M., Lane reservation for highways (position paper), in 2007 IEEE Intelligent Transportation Systems Conference, pp. 795-800, 2007.
21. Razzaque M. A., Ghaleb F. A., and Zainal A., Mobility Pattern Based Misbehavior Detection to Avoid Collision in Vehicular Adhoc Networks, in International Conference on Ubiquitous Computing and Ambient Intelligence, pp. 300-303, 2014.
22. Raw M. K. RS., Singh N., Security issues and solutions in Vehicular Ad hoc Network: A review approach, 2013.
23. Rezgui J. and Cherkaoui S., Detecting faulty and malicious vehicles using rule-based communications data mining, in Local Computer Networks (LCN), 2011 IEEE 36th Conference on, pp. 827-834, 2011.
24. Rohini Nere U. N., Security Of Broadcasting Protocols In Vanet, International Journal of Grid Computing & Applications (IJGCA), vol. 6, pp. 13-25,2015.
25. Rupareliya J., Vithlani S., and Gohel C., Securing VANET by Preventing Attacker Node Using Watchdog and Bayesian Network Theory, Procedia Computer Science, vol. 79, pp. 649-656, 2016.
26. Soomro I. A. and Hasbullah H., User requirements model for vehicular Ad hoc network applications, in 2010 International Symposium on Information Technology, pp. 800-804, 2010.
27. Van der Heijden R., Dietzel S., and Kargl F., Misbehavior detection in vehicular ad-hoc networks, Ph. D. Thesis, Kumaun University, Nainital, India, 2013.
28. Vulimiri A., Gupta A., Roy P., Muthaiah S. N., and Kherani A., Application of secondary information for misbehavior detection in vanets, in International Conference on Research in Networking, pp. 385-396, 2010.
29. Wahab O. A., Otrok H., and Mourad A., A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles, Computer Communications, vol. 41, pp. 43-54, 2014.
30. Wahab O. A., Otrok H., and Mourad A., VANET QoS-OLSR: QoS-based clustering protocol for Vehicular Ad hoc Networks, Computer Communications, vol. 36, pp. 1422-1435, 2013.
31. Wahab O. A., Mourad A., Otrok H., and Bentahar J., CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks, Expert Systems with Applications, vol. 50, pp. 40-54, 2016.
32. Wang Z, Chigan C., Countermeasure uncooperative behaviors with dynamic trust-token in VANETs, IEEE International Conference on Communications, pp. 3959-3964, IEEE, 2007.

1/25/2017