Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 965 – 972

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks

Uzma Khan[a,*], Shikha Agrawal[a], Sanjay Silakari[a]

[a]*University Institute of Technology, RGPV, Bhopal (M.P.) 462036, India*

Abstract

VANETs enable wireless communication among vehicles and vehicle to infrastructure. Its main objective is to render safety, comfort and convenience on the road. VANET is different from ad-hoc networks due to its unique characteristics. However, because of lack of infrastructure and centralized administration, it becomes vulnerable to misbehaviors. This greatly threatens different aspects of VANET's security. VANET being such a useful network must provide adequate security measures for secure communication. The proposed algorithm DMN-Detection of Malicious Nodes in VANETs improves DMV Algorithm in terms of effective selection of verifiers for detection of malicious nodes and hence improves the network performance.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Malicious; Misbehaviour; Detection; Security;Performance; Vehicular Ad-Hoc Networks (VANETs).

1. Introduction

Traditional wired networks have mechanism for protection by various means of defence like gateways, firewalls etc. However, wireless networks are susceptible to security attacks targeting almost the entire network from any direction. Therefore, VANETs being an Ad-hoc Network are at risk of various misbehaviours like tampering of messages, eavesdropping, spamming, masquerading etc because of lack of centralized administration [1, 5, 21]. Security

* Corresponding author. Tel.: +91 8878881518.
E-mail addresses:uzma.khancs@gmail.com, shikha@rgtu.net, ssilakari@yahoo.com

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.01.006

of VANETs has been identified as one of the major challenge[8]. 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 [3, 22, 23].

Different misbehavior detection schemes have been proposed by researchers in order to identify the attackers responsible for misconducts in VANETs. Detection of such malicious nodes and abnormal activities in the network is very significant in order to devise precautionary measures for it. This paper proposes a node centric detection scheme called DMN (Detection of Malicious Nodes) which effectively detects malicious nodes that drop and duplicate packets in the network using monitoring approach. Nodes are being monitored by the verifiers which qualify the selection threshold. Thus, instead of selecting all the trustworthy nodes, only the most suitable nodes perform the job of monitoring other node's behavior. This helps to utilize the network resources properly which is generally overlooked by the researchers in their detection schemes. This, in turn improves the network performance which is one of the major requirement of security schemes for complex networks like VANETs.

The paper is organized as follows: Section 2 discusses the various node-centric and data-centric techniques for detecting misbehavior and malicious nodes in VANETs. Section 3 presents the DMN algorithm in detail. Performance evaluation and its comparative analysis are discussed in Section 4. Conclusion and Future work are stated in Section 5.

2. Related Work

Number of schemes has been proposed to detect misbehavior and malicious nodes in Vehicular Ad-hoc Networks. The misbehavior detection schemes can be broadly classified into following two types: Node-centric and Data-centric misbehavior detection schemes.

2.1. 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.

In the research work [9, 10], Gosh et al. have proposed a robust scheme to detect malicious vehicles for Post Crash Notification application. They have considered the possibility of the fake position information of the vehicle in the PCN along with the false crash alert in [10]. Kim et al.[6] 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 vehicular ad-hoc networks. Daeinabi et al.[3] have proposed a detection algorithm called DMV to discover malicious nodes through observations that duplicates or drops received packets and isolates such vehicles from honest nodes. Vehicles are tagged using a distrust value and are monitored by the allocated verifier nodes. Wahab et al.[16] have used Quality of Service-Optimized Link State Routing (QoS-OLSR) clustering algorithm to detect malicious vehicles in (VANET) using Dempster–Shafer based cooperative watchdog model. This method maintains stability and quality of service with increase in detection probability and decreases the number of selfish nodes and false negatives. Kadam et al. have presented a new approach[14] for not solely the detection of malicious vehicles attack, additionally their prevention from the VANET. It is an improvement of the Detection of Malicious Vehicles (DMV) algorithm [3]. This approach reduced the impact of black hole attack within VANET and is more efficient and secure compared to DMV.

2.2 Data Centric Misbehavior Detection Schemes

Data-centric approach inspects the data transmitted among nodes to detect misbehaviors. 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. Few research contributions to the data-centric misbehavior detection scheme are as follows.

In the research work[2], Vulimiri et al. have detected misbehavior in VANETs based on the secondary information or alerts that are created in response to the primary alerts for PCN application. A new misbehavior detection scheme introduced by Ruj et al.[20] used the idea of data-centric misbehavior detection algorithmic program. Fake alert messages and misbehaving nodes are detected by monitoring the actions of the vehicle after alert messages have been sent. To be able to find the malicious vehicle, Rezgui et al.[18]developed a mechanism VARM that collects, at one vehicle, information relating to every neighbor transmission. Rawat et al.[17] have proposed a novel algorithm to secure the communication in the Vehicular Ad-hoc Network by detecting malicious driver using a probabilistic approach. It computes the trust of the messages received and checks whether the message is from an honest vehicle or not. Grover et al.[12] have presented a security framework in order to categorize numerous misbehaviors in VANET using machine learning technique. It differentiates a malicious node and an honest node based on the features computed by the observer nodes. Grover et al.[13] presented a security framework for detection of misbehaviors in VANETs using an ensemble primarily based machine learning approach. Based on misbehavior detection systems, running on vehicles and roadside infrastructure units, a central evaluation system[15] is presented that aims to spot and exclude attackers from the network. In the research paper[4], Barnwal et al. have presented a short term misbehavior detection scheme which can detect a malicious node that is spreading fake position and speed information through its heartbeat/beacon messages. Harit et al.[11] have presented a scheme based on the data centric approach which detects the correctness of the information received, primarily for PCN alerts. It makes use of a Fox-Hole region which helps to find the safety value of any vehicular node on its current location and present speed. In the paper [7], Huang et al. have proposed a cheater detection protocol which detects malicious vehicles that broadcast fake congestion information in the network for their selfish motives and impersonate other 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. Coussement et al. [19] have proposed an Intrusion detection system (IDS) which is capable of detecting malicious activities made to the system. A decision support protocol is designed for security in VANETs which verifies the signature of the incoming and outgoing packets.

3. Network Model and Definitions

VANET consists of vehicles and Road Side Units (RSUs) that communicate with each other using short range radio communication. In order to provide authentication and security, there are third parties in VANETs called Certificate Authorities (CAs). CAs are responsible for management of identities of the vehicles in the network and verifying the misbehavior reports sent by the verifier nodes and if found true, modifying the distrust value of nodes accordingly. Each vehicle has a white list provided by its respective cluster head and a black list containing list of malicious nodes sent by CA.

3.1 Algorithm Description

The Detection of Malicious Node (DMN) algorithm is based on the following three basic concepts -

- A vehicle is considered to show an abnormal behavior if it drops or duplicate the packets received to it so as to create congestion in the network, misguide other vehicular nodes or destroy crucial messages for their selfish motives.
- An honest vehicle forwards the messages received to it correctly to other nodes in the network or creates right messages for transmission.
- A vehicle will be tagged as a malicious vehicle, if the vehicle repeats abnormal behavior such that its distrust value, D_V exceeds the threshold value T_{MD}.

3.2 Detection of Malicious Nodes in Vehicular Ad-hoc Networks – DMN Algorithm

In VANET communication, a node acts as a source which is the generator of the information. There is another node which acts as a destination of the message, and other intermediate nodes between source and destination acts

as relay nodes. When a vehicular node V_N plays the role of a relaying node, other trustier vehicles which are its verifiers, monitors its behaviour. When vehicleV_U works as a verifier of V_N, it checks the number of packets received by V_N (represented by parameter a) and number of packets that V_N drops or duplicates as detected by V_U (represented by parameter b). After a particular time has elapsed P_L, if vehicle V_N does not send forward a received packet or sends its multiple copies, it is considered as abnormal behaviour by verifier V_U and hence increases the value of parameter b by 1 unit. The parameter D_V (distrust value) is associated with each vehicle and changes when an abnormal behaviour is observed. The new distrust value is informed to all neighbours and they update their lists accordingly. Vehicles cooperate with one another while they are part of the white list as their Dv is lower than the threshold. If it exceeds the threshold, the ID of the vehicle is reported to the CA as a malicious node. CA then broadcasts the ID of malicious node to all others nodes.

In the proposed Detection of Malicious Nodes (DMN) algorithm, verifier is selected on the basis of the parameters: distrust value, load, and distance. Those nodes are selected as verifier whose Decision parameter, D_P is less than the Selection Threshold, T_{VS} among other neighbouring nodes located in the region r (CH, V_N). This approach optimizes the selection of verifier nodes and thus helps to save the network bandwidth and hence improves network performance.

Nodes in the region r are considered for being verifiers. The region r denotes the intersection area of vehicular node V_N and its CH. Area of CH refers to its transmission range and area of vehicle V_N is calculated by the formula given below in Eq (1). Thus it ensures all verifiers are able to send misbehaviour reports to the CH.

$$\textbf{Area } (V_N) = T_R(V_N) - P_L \ (Smx - Smn) \quad (1)$$

where,

$T_R(V_N)$ - Transmission range of vehicle V_N.

P_L- Packet latency in vehicles.

S_{mx} - Maximum speed of vehicle.

S_{mn} - Minimum vehicle's speed

The parameters for selection of verifiers in the area r are explained below:

- **Load (L_D)** - It refers to the number of nodes, a vehicle is already monitoring. It is considered so as to balance the monitoring job among the nodes. Thus a node which has less load compared to others will have greater chance to be selected as verifier.
- **Distrust value (D_V)** – It refers to the measure of trustworthiness of a vehicle. It means less the distrust value, more trustworthy a node is. If a vehicle shows abnormal behaviour, this value is increased and compared to the threshold for making appropriate decisions i.e a vehicle should remain in the white list or tagged as a malicious vehicle and moved to the black list.
- **Distance (D_S)** – If the distance of a node from the vehicle to be monitored is less, then the node will remain in the transmission range of the vehicle for a longer time. Thus, this provides scope for better observations and decision making.

Decision Parameter, D_P is calculated for all the nodes considered for verifier selection by taking into account the load, distance and distrust value of the node by the following equation (2).

$$D_P = W_1 * L_D + W_2 * D_V + W_3 * D_S \quad (2)$$

where, W_1, W_2, and W_3 are the weight factors for parameters Load (L_D), Distrust Value (D_V) and Distance (D_S) respectively such that,

$$W_1 + W_2 + W_3 = 1 \quad (3)$$

Instead of selecting all the nodes with smaller distrust value than the vehicular node V_N, allocating few nodes as verifiers which are more appropriate for monitoring process helps in better detection of malicious nodes as well as improves network performance. As few nodes perform the job of monitoring the node V_N, this saves network resources used for reporting the behaviour and conserve their time for processing the observed behaviour for all the nodes. As the network utilization is enhanced, it results in better transmissions in the network. In order to assign verifiers for the node V_N, the decision parameter D_P calculated for the nodes under consideration is compared to the

Selection Threshold T_{VS}. If a node's decision parameter value is less than the selection threshold ($D_P < T_{VS}$), then the vehicle is allocated as verifier. This way proposed approach optimizes the selection of verifier nodes.

Vehicles know the distrust value of other vehicles present in its neighbourhood. When a vehicle V_U reports an abnormal behaviour of another vehicle V_N, CH verifies the D_V of V_U to make sure that it is lower or equal to the D_V of V_N. CH is considered to be the most reliable and trustworthy node within a cluster. Thus, verifiers for an honest node are not assigned among the vehicles which show abnormal behaviour as such vehicles have greater D_V as compared to a normal node. In case, CH is found to misbehave then it is being replaced by a trustier vehicle. Thus, the process consists of all aspects of monitoring the vehicles in order to identify the malicious nodes. In addition, it also improves the selection of verifiers by the proposed approach which results in better network utilization and enhanced performance.

3.3 Proposed DMN Algorithm

Step 1: Vehicle V_N joins the vehicular network.
Step 2: Get the cluster keys.
Step 3: Compute the parameters- Load, Distrust Value and Distance for the nodes in area of V_N for verifier selection.
Step4: Calculate the Decision parameter for verifier selection, D_P.
$\mathbf{D_P = W_1 * L_D + W_2 * D_V + W_3 * D_S}$
Where,
$\mathbf{W_1 + W_2 + W_3 = 1.}$
W1, W2, and W3 are the weight factors for parameters Load (L_D), Distrust Value (D_V) and Distance (D_S) respectively.
Step 5: Find out nodes with Decision parameter value less then Selection Threshold, i.e
$\mathbf{(D_P < T_{VS})}$
Step 6: Allocate nodes obtained from Step 5 as verifiers to the recently joined vehicle V_N.
Step 7: Verifiers monitor behavior of vehicle V_N.
Step 8: If (verifier detects vehicle V_N showing abnormal behavior)
Report to the cluster head (CH)
goto step 9;
else
goto step 7;
Step 9: CH calculates new distrust value (D_V) of V_N.
Step 10: If distrust value is less than or equal to detection threshold i.e
if ($D_V <= T_{MD}$) then
update the white list and goto 7
else
goto 11
Step 11: Warning message is send to all other nodes.
Step 12: Update the entry of Vehicle V_N in black list.
Step 13: Isolate the detected malicious vehicle from the network.

4. Performance Evaluation

To analyze the performance of the proposed algorithm Detection of Malicious Nodes in Vehicular Ad-hoc Network (DMN), we have performed the simulation in Network Simulator -2. The weight factor for load, distance and distrust value for the computation of decision parameter are taken as 40%, 30% and 30% respectively. The performance of the proposed DMN algorithm is computed in terms of Packet Delivery Ratio, Average End to End Delay and Throughput. The simulation parameters used for performance evaluation of DMN and DMV algorithm are shown in the Table 1.

Table 1.Simulation Parameters.

Parameter	Value
Number of Nodes	50
Traffic Pattern	CBR (Constant Bit Rate)
Network Size	2500x50
Simulation Time	100s
Speed of Vehicles	70-120 km/hr
Packet Transmission Rate	5 packets/s
Number of Malicious Nodes	5,8,10,25

4.1 Performance Metrics

In order to measure the performance of our proposed DMN algorithm, following performance parameters are evaluated in comparison to DMV.

Average Throughput - The amount of data transferred per unit time or average rate of successful message transmissions per sec over a communication channel is known as throughput. It is generally measured in bits per second (bits/s or bps).

Throughput= (Total Received Packets) / ((Stop Time –Start Time)) (4)

Packet Delivery Ratio - Packet delivery ratio is the metrics that calculates the ratio of data packets received by the destination nodes to those produced by the source nodes.

Packet Delivery Ratio = (Data Packet Received by the Destinations)/(Data Packet Generated by the Sources) (5)

End to End Delay - End to End Delay is the time between the origination of packet at the source and packet delivery time at the destination. If any data packet is lost or dropped during the transmission, then it will not be considered for the metrics calculation

End to End Delay = Packet Delivery Time at Destination - Packet Origination Time at Source (6)

Fig. 1., Fig. 2., and Fig. 3. given below shows comparative analysis of above metrics of DMN and DMV.

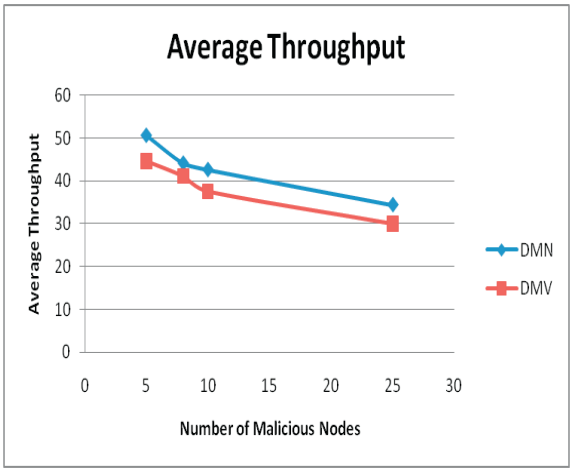

Fig. 1. Comparative Analysis of Average Throughput of DMN & DMV

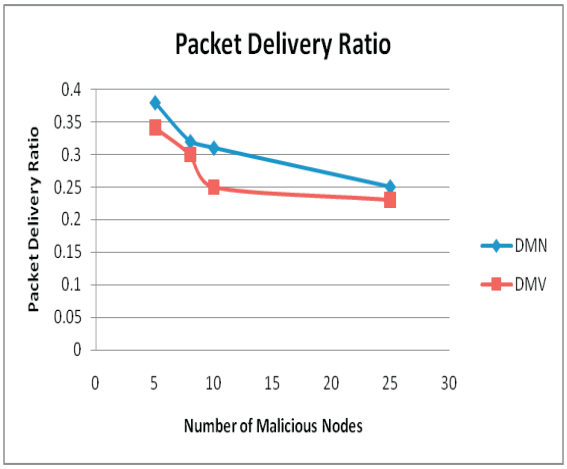

Fig. 2. Comparative Analysis of Packet Delivery Ratio of DMN and DMV

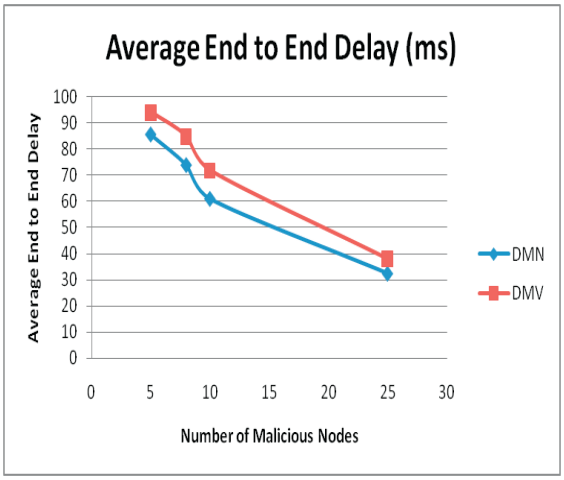

Fig. 3. Comparative Analysis of Average End to End Delay of DMN and DMV

From the results obtained, it can be analyzed that DMN improves network performance of DMV by optimizing the selection of verifier nodes. It shows better results than DMV, in terms of Average Throughput, Packet Delivery Ratio and End to End Delay.

5. Conclusion and Future Work

To effectively detect misbehaviours and malicious vehicular nodes in VANETs, we have proposed a novel algorithm called DMN (Detection of Malicious Nodes in VANETs). DMN algorithm is designed to isolate the nodes showing abnormal behaviour as well as enhancing the network performance. DMN optimizes the selection of verifier nodes which perform the work of monitoring node's behaviour. DMN improves the pre-existing DMV algorithm which selects all the nodes as verifiers which have distrust value less than the vehicle to be monitored. It has been optimized by our proposed DMN algorithm taking into consideration three parameters for choosing appropriate verifiers that are load, distance and distrust value. Based on these parameters, a decision value is evaluated and compared to verifier selection threshold. Thus, optimal verifier selection improves the network

utilization and in turn improves network performance. The simulation results indicates that DMN provides higher throughput, better packet delivery ratio and reduces the end to end delay, when compared to DMV algorithm. In order to further enhance the proposed DMN approach, we will consider other optimization techniques like PSO to select verifiers in the algorithm. Complex traffic and mobility modelling can be considered in our simulation framework and can be evaluated in different scenarios. The proposed work can be extended with a prevention technique for the malicious nodes. Also deploying the proposed method in real time will help to test and analyze its performance under realistic conditions.

References

1. Al-kahtani, MS. Survey on security attacks in Vehicular Ad hoc Networks (VANETs). In: *6th International Conference on Signal Processing and Communication Systems (ICSPCS);* 2012. p. 1-9.
2. Vulimiri A, Gupta A, Roy P, Muthaiah SN, Kherani AA. Application of Secondary Information for Misbehavior Detection in VANETs. *Springer, IFIP, LNCS* 2010. **6091**: 385-396.
3. Daeinabi A, Rahbar AG. Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks. *Springer, Multimedia Tools and Applications* 2013. **66**: 325-338.
4. Barnwal RP, Ghosh SK. Heartbeat Message Based Misbehavior Detection Scheme for Vehicular Ad-hoc Networks. In: *International Conference on Connected Vehicles and Expo (ICCVE)* 2012; p. 29-34.
5. Mishra B, Nayak P, Behera S, Jena D. Security in vehicular adhoc networks: a survey. *ACM, ICCCS;* 2011. p. 590-595.
6. Kim CH, Bae IH. A Misbehavior based reputation management system for vanets. *Springer, LNEE* 2012. **181**: 441-450.
7. Huang D, Williams SA, Shere S. Cheater Detection in Vehicular Networks. In: *11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*; 2012. p.193-200.
8. Fonseca E, Festag A. A survey of existing approaches for secure ad hoc routing and their applicability to VANETs. *NEC Network Laboratories;* 2006.
9. Ghosh M, Varghese A, Gupta A, Kherani AA, Muthaiah SN. Detecting misbehaviors in VANET with integrated root-cause analysis. *Elsevier Ad Hoc Network*, 2010; **8**:778–790.
10. Ghosh M, Varghese A, Kherani AA, Gupta A. Distributed Misbehavior Detection in VANETs. *Wireless Communications and Networking Conference* 2009; p.1-6.
11. Harit SK, Singh G, Tyagi N. Fox-Hole Model for Data-centric Misbehaviour Detection in VANETs. *In: Third International Conference on Computer and Communication Technology (ICCCT),* 2012; p. 271-277.
12. Grover J, Prajapati NK, Laxmi V, and Gaur MS. Machine Learning Approach for Multiple Misbehavior Detection in VANET. *Springer, CCIS, 2011*; **192**: 644-653.
13. Grover J, Laxmi V, Gaur MS. Misbehavior Detection Based on Ensemble Learning in VANET. *Springer, LNCS, ADCONS*, 2011; **7135**: 602-611.
14. Kadam M, Limkar S. Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map. *AISC Springer* 2014; **247**: 379–387.
15. Bißmeyer N, Njeukam J, Petit J, Bayarou KM. Central Misbehavior Evaluation for VANETs based on Mobility Data Plausibility. *ACM VANET'12*, 2012.
16. Wahab OA, Otrok H, Mourad A. A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles. *Elsevier, Computer communications* 2014; **41**: 43-54.
17. Rawat DB, Bista BB, Gongjun Y, Weigle MC. Securing Vehicular Ad-hoc Networks Against Malicious Drivers: A Probabilistic Approach. In: *International Conference on Complex, Intelligent and Software Intensive Systems (CISIS);* 2011. p. 146-151.
18. Rezgui, J.; Cherkaoui, S. Detecting faulty and malicious vehicles using rule based communications data mining. In: *36th Conference on Local Computer Networks (LCN), IEEE;* 2011. p. 827-834.
19. Coussement R, Saber BAB, Biskri I. Decision support protocol for intrusion detection in VANETs. *ACM, DIVANet '13*; 2013. p. 31-38.
20. Ruj S, Cavenaghi MA, Huang Z, Nayak A, Stojmenovic I. On Data-Centric Misbehavior Detection in VANETs. In: *Vehicular Technology Conference (VTC Fall), IEEE*; 2011. p.1-5.
21. Liu Y; Bi J, Yang J. Research on Vehicular Ad Hoc Networks. In: *Control and Decision Conference*; 2009. p. 4430-4435.
22. Isaac JT, Zeadally S, Camara JS. Security attacks and solution for Vehicular ad hoc Networks, *IET communication* 2010; **4**: 894-903.
23. Hussain R, Son J, Oh H. Anti Sybil: Standing against Sybil attacks in privacy preserved VANETs. In: *International Conference on Connected Vehicles and Expo*, *IEEE*; 2012. p. 108-113.