Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

MONITORING OF VEHICULAR AD-HOC NETWORKS TO DETECT MALICIOUS VEHICLES (DMV)

Garima Saini[1] and Dinesh Javalkar[2]

1 Research Scholar, Lingayas Vidyapeeth, Faridabad
2 Asst. Professor Lingayas Vidyapeeth, Faridabad

1. INTRODUCTION

Traditional wired networks are protected by various defence mechanisms such as gateways and firewalls. Wireless networks, on the other hand, are vulnerable to security threats that can threaten the entire network from either direction. Because of the lack of centralised administration, VANETs, As an ad hoc network, different misconducts such as messages manipulation, eavesdropping are vulnerable, spamming, masquerading, and so on (Al-kahtani. MS. 2012)(Mishra B, et al.,2011) (Liu Y et al.,2009)..[1] ,[5] [21] One of the major challenges has been described as the security of VANETs. VANET applications permit ongoing correspondence and handle life-basic data. To secure against aggressors and noxious vehicular hubs, it should stick to security principles like genuineness, secrecy, namelessness, non-disavowal, and verification.

Researchers have suggested various misbehaviour identification systems to arrange the assailants liable for offense in VANETs. The identification of such malignant hubs and dubious organization movement is basic to define precaution measures. DMN (Detection of Malicious Nodes) is a hub driven identification plot proposed in this paper that viably identifies malevolent hubs that drop and copy parcels in the organization utilizing an observing strategy. The verifiers who qualify the choice edge watch out for the nodes. As an outcome, as opposed to picking the entirety of the dependable hubs, just the most suitable hubs play out the undertaking of checking the activities of different hubs. This guides in the appropriate utilization of organization assets, which is frequently disregarded by scientists in their location

Article to Cite:
Garima Saini & Dinesh Javalkar. (2021). Monitoring of vehicular ad-hoc networks to detect malicious vehicles (DMV), Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition), 40(6).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

schemes. As an outcome, network proficiency expands, which is a vital necessity of protection schemes for complex networks like VANETs.(Daeinabi A et al.,2013)(Isaac JT, et al.,2010) (Hussain et al.,2012)[3],[7]

2. SIGNIFICANCE OF THE STUDY

Nowadays VANET occupies a major role in the intelligent Transportation System (ITS) which is connected with Cyber Physical System (CPS). Because of this a huge research gap is created in designing a secured VANET networks. An effective communication system for VANETs is very essential to protect the network from the vulnerabilities. And on the other side the increased vehicular traffic leads to roadside accidents. So there is a need of intelligent vehicle system which can act smartly during the emergency situation compared with the normal condition.

3.REVIEW OF RELATED STUDIES

In Vehicular Impromptu Organizations, various plans have been proposed to identify trouble making and malignant hubs. The accompanying two types of mischief ID frameworks might be barely ordered: There are two kinds of bad conduct recognizable proof plans: hub driven and information driven. Recognition Plans for Hub Driven Mischief Verification is utilized in hub driven strategies to separate between different hubs. To verify the hub moving the parcel, security qualifications, computerized marks, and different strategies are utilized. The hubs communicating the messages, as opposed to the information moved, are the focal point of such plans. Gosh et al. recommended a complete plan to distinguish malevolent vehicles for the Post Accident Warning application in their examination paper (Ghosh M et al.,2010),(Ghosh M et al.,2009). [9] ,[10]. They considered the likelihood of a vehicle's phony area subtleties in the PCN, just as a bogus accident cautioning in (Ghosh M et al.,2009). (Kim. CH et al.,2012)[10] [6] presented another Mischief Based Standing Administration Plan (MBRMS) that comprises of three areas. For the ID and filtration of bogus data in vehicular specially appointed organizations, there are three algorithms:

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

a) Rowdiness discovery,

b) Occasion rebroadcast

c) Worldwide expulsion calculations.

Daeinabi et al. [3] proposed the DMV discovery calculation to recognize vindictive hubs by seeing how they rehash or drop got bundles and disengage them from legit hubs.

Vehicles are set apart with a question esteem and followed by the verifier hubs doled out to them. (Wahab. OA et al.,2014) [16] utilized a DempsterShafer based helpful guard dog model to identify noxious vehicles in a VANET utilizing the Nature of Administration Advanced Association State Directing (QoS-OLSR) grouping calculation. With an improvement in recognition likelihood, this methodology jam administration unwavering quality and productivity while decreasing the quantity of egotistical hubs and bogus negatives. (KadamM et al.,2014)[14] have proposed another methodology for recognizing malignant vehicles assaults as well as keeping them from entering the Vehicular Ad hoc Network. It is an improvement to the Acknowledgment of DMV algorithm (Daeinabi A et al.,2013)[3] . This technique limited the effect of a dark opening assault inside the VANET and is more powerful and stable than DMV.

3.1 Data-Centric Misconduct Detection Methodologies

To distinguish mischievous activities, an information driven methodology investigates the information sent between nodes.It is more worried about interfacing a larger number of communications compared to the people who operate the individual hubs. The information that is disseminated by the organization's hubs is assessed and contrasted with the data acquired by different hubs to decide the best course of action.Verify the exactness of the got notice messages.

Coming up next are a couple of exploration commitments to the information driven misconduct recognition plot.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

In the research work, (Vulimiri A, et al.,2010)[2] (have discovered trouble making in VANETs dependent on the auxiliary data or admonitions that are made in light of the essential alarms for PCN application..(Ruj. S,et al.,2011) [20] proposed a new misbehaviour detection system based on a data-centric misbehaviour detection algorithmic programme.After warning messages have been received, the vehicle's activities are monitored to detect fake alert messages and misbehaving nodes..(Rezgui.J et al.,2011)[18] created VARM, a mechanism that gathers information about any neighbour transmission at a single vehicle in order to locate the malicious vehicle..(Rawat. DB et al.,2011)[17] recommended a novel calculation to get correspondence in the Vehicular Specially appointed Organization by utilizing a probabilistic technique to distinguish noxious drivers.It calculates the message's trustworthiness and determines if the message came from a trustworthy vehicle.(Grover.J et al.,2011)[13] have proposed a security system that uses machine learning to categorise a variety of VANET misbehaviors. In light of the highlights processed by the eyewitness hubs, it recognizes malevolent and legit hubs..(Grover.J et al.,2011) [13] utilized a group fundamentally based AI way to deal with present a security structure for identifying mischievous activities in VANETs.

A focal appraisal system15 dependent on bad conduct recognition frameworks working on vehicles and side of the road foundation units is introduced, fully intent on distinguishing and barring assailants from the network.Barnwal et al. presented a momentary rowdiness location plot in their examination paper4 that can recognize a pernicious hub.(Harit.SK et al.,2012)[11] have proposed a plan zeroed in on an information driven methodology for distinguishing the accuracy of got data, basically deciding the security worth of any vehicular hub dependent on its present position and speed.Huang et al. proposed a con artist distinguishing proof convention in paper (Huang.D.et al.,2012)[7] that recognizes vindictive vehicles that transmission counterfeit clog data in the organization for their own narrow minded reasons and imitate other non-existing vehicles.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

In this case, radar estimates of surrounding speed and distance are used to confirm the occurence of a blockage that was generated by a vehicle hub.

In an IDS designed to detect malevolent attacks, the team (Coussement, et al., 2013)[19] proposed that the system be able to self-diagnose. Convention developed to aid secure transportation networks in VANETs provides an option for each arriving and active parcel to be identified and verified.

3. 2 Definitions and Models of Networks

Vehicles and Street Side Units (RSUs) speak with one another through short-range radio correspondence in the VANET.Certificate Specialists are outsider elements that give verification and assurance in VANETs (CAs).

CAs are responsible for dealing with the characters of the vehicles in the organization, just as checking bad conduct .Each vehicle has a white summary given by its gathering head, similarly as a blacklist containing an overview of malignant center points given by CA.

4. DESCRIPTION OF THE ALGORITHM

The three fundamental rules that the Location of Noxious Hub calculation depends on are:

1. A vehicle is considered to be acting unusually on the off chance that it drops or copies parcels shipped off it to cause network clog, mislead other vehicular hubs, or erase basic directives for individual addition.

2. A legitimate vehicle sends the messages it gets to different hubs in the organization in the right request or produces the right directives for transmission.

3. A vehicle will be marked vindictive on the off chance that it displays dubious movement regularly enough that its question esteem, DV, surpasses the edge esteem TMD.

Vindictive Hub Location in Vehicular Impromptu Organizations - DMN Calculation

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

In VANET correspondence, a hub fills in as a source, or the information generator. Another hub fills in as the message's objective, and there are moreover middle hubs between the source and the objective. as hubs that hand-off data When a vehicular hub VN goes about as a handing-off hub, it is observed by other confided in vehicles that go about as verifiers. VehicleVU tests the quantity of parcels got by VN (addressed by boundary a) and the quantity of bundles that VN drops or copies as seen by VU when going about as a VN verifier (addressed by boundary b).

In the event that, after a specific measure of time has passed PL, vehicle VN neglects to advance a got parcel or sends a few duplicates of it, verifier VU believes this to be sporadic conduct and raises the worth of boundary b by one unit. Every vehicle has a boundary called DV (doubt esteem), which changes when unusual conduct is distinguished. The two neighbors are recounted the new question esteem, and their rundowns are refreshed as needs be.

When on the white rundown, vehicles consent to each other in light of the fact that their Dv is not exactly the limit. On the off chance that it arrives at the edge, the vehicle's ID is hailed as a malevolent hub by the CA. The vindictive hub's ID is then transmission to any remaining hubs by CA. The verifier in the proposed Recognition of Vindictive Hubs (DMN) calculation is picked dependent on three boundaries: question significance, burden, and degree.

Those hubs in the area r are picked as verifiers whose Choice boundary, DP, is not exactly the Choice Edge, TVS, among other close by hubs (CH, VN). This technique streamlines the choice of verifier hubs, bringing about network transfer speed reserve funds and improved organization effectiveness.

Nodes in the r region are thought to be verifiers.

The crossing point space of vehicular hub VN and its CH is indicated by the locale r. The transmission scope of a vehicle is characterized by its space, and the space of a vehicle VN is resolved utilizing the recipe in Eq (1). Thus, the two verifiers will report mischief to the CH.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

Region (VN) = TR(VN) – PL (Smx - Smn) (1)

where,

TR(VN) - Transmission scope of vehicle VN.

PL- vehicle's Parcel inactivity.

Smx – vehicle's Greatest speed .

Smn–Least Speed of vehicle

The boundaries for choice of verifiers in the space r are clarified beneath:

(L_D) – Also known as load. It refers to the number of hubs that are observed by a vehicle. The check position between the hubs is adapted. This is considered. Afterwards, a hub with less burden than others have a more significant opportunity to be selected as a verifier.

(D_V) - Also known as Distrust value. The fraction of the vehicle's trustworthiness is referred to. It means less esteem for doubt, more trustworthy is a hub. Should a vehicle exhibit an odd behavior, that value is also increased, as opposed to the limit for fitting options, i.e., a car should stay a white summary or a vehicle called dangerous and be placed to the blacklist.

(D_S) - Also known as Distance. If the distance between a hub and the vehicle is smaller, the hub will remain in the vehicle transmission range at this point for a time frame that is more precise. This therefore leads to improved perceptions and dynamics.

DP is defined by the heap, distance, and doubt of the hub by the following conditions for each of the hubs examined for verifier choice. (2).

DP = W1 * LD + W2 * DV + W3 * DS(2)

where, W1, W2, and W3 are the weight factors for boundaries Burden (LD), Doubt Worth (Dv) and Distance (DS) individually to such an extent that,

W1+W2+W3 =1(3)

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

Rather than choosing every one of the hubs with more modest doubt esteem than the vehicular hub VN, distributing not many checking measure helps in better revelation of toxic centers similarly as improves network execution. As couple of hubs play out the work of observing the hub VN, this saves network assets utilized for announcing the conduct furthermore, moderate their time for handling the noticed conduct for every one of the hubs. As the organization usage is improved, it brings about better transmissions in the organization.

This technique increases the selection of verifier emphasis. Cars understand the value of the vulnerability of various vehicles around. In particular, CH insists on the VU DV when a VU vehicle reports an odd direct from another VN vehicle that it is lower or indistinguishable from the VN DV. CH is seen as the strongest and most reliable focus of a social opportunity. Thereafter, checkers for an authentic focus point are not allocated to vehicles that are odd immediately as such cars have higher observable DVs when shown to match a conventional focus point. Chances that, CH is displaced by a truster vehicle are determined to be pernicious. As needed, the participants see the vehicles in all directions to perceive the focus on poison. In addition, the proposed technique enhances the determination of verifiers, which improves the usage of membership and re-designs implementation.

Stage 2: Get the gathering keys.

Stage 3: Register the boundaries Burden, Doubt Worth and Distance for the hubs in space of VN for verifier choice.

Step4: Compute the Choice boundary for verifier determination, DP.

DP = W1 * LD + W2 * DV + W3 * DS

Where,

W1 + W2 + W3 = 1.

W1, W2, and W3 are the weight factors for boundaries Burden (LD), Doubt Worth (DV) and Distance (DS) separately.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

Stage 5: Discover hubs with Choice boundary esteem less then Choice Edge, i.e

(DP < TVS)

Stage 6: Apportion hubs got from Stage 5 as verifiers to the as of late joined vehicle VN.

Stage 7: Verifiers screen conduct of vehicle VN.

Stage 8: If (verifier recognizes vehicle VN showing unusual conduct)

Report to the group head (CH)

goto stage 9;

else

goto stage 7;

Stage 9: CH ascertains new doubt esteem (DV) of VN.

Stage 10: If doubt esteem is not exactly or equivalent to discovery edge i.e

assuming (DV < = TMD)

update the white rundown and goto 7

else

goto 11

Stage 11: Cautioning message is ship off any remaining hubs.

Stage 12: Update the passage of Vehicle VN in boycott.

Stage 13: Detach the recognized noxious vehicle from the organization.

5. PERFORMANCE EVALUATION

We used Network Simulator -2 to reproduce the proposed calculation Identification of Malevolent Hubs in Vehicular Specially appointed Organization (DMN) and assess its exhibition. For the calculation of the choice boundary, the weight factors for burden, distance, and doubt esteem are set to 40%, 30%, and 30%, individually. The

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

proposed DMN calculation's proficiency is estimated as far as Bundle Conveyance Proportion, Normal Finish to End Deferral, and Throughput. Table 1 shows the reproduction boundaries used to assess the productivity of the DMN and DMV calculations.

Sr. No	**Parameter**	**Value**
1	No. of Nodes	50 , 100 , 200
2	Traffic Pattern	TCP/FTP, UDP/CBR
3	Network Size	2500×50 , 2000×100
4	Simulation Time	100 sec
5	Speed of Vechicles	70-120 km/hr
6	Packet transmission rate	5 packets/sec
7	Number of Malicious Nodes	5,8,10,25

Table 1.Simulation Parameters.

Metrics of Performance

The accompanying yield boundaries are contrasted with dmv to evaluate the exhibition of our proposed dmn calculation. normal throughput - throughput is characterized as the measure of information sent per unit of time or the normal pace of compelling message transmissions each second over a correspondence channel. bits each second (bits/s or bps) is the most widely recognized unit of measurement.(total got bundles)/((stop time - start time)) = throughput (four) parcel conveyance proportion - this measurement estimates the proportion of information bundles gotten by objective hubs to those produced by source hubs. parcel conveyance proportion = (information bundles got by objections)/(information bundles got by objections)/(information bundles got by objections)/(information parcel created by the sources) (no. 5) . start to finish delay - the period between bundle beginning at the source and parcel appearance time at the objective is known as start to finish delay. in the event that an information parcel. bundle conveyance time at objective - parcel beginning time at source = start to finish delay (6).imilar

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

investigation of the above measurements of dmn and dmv is appeared in figure 1, figure 2, and figure 3**.**

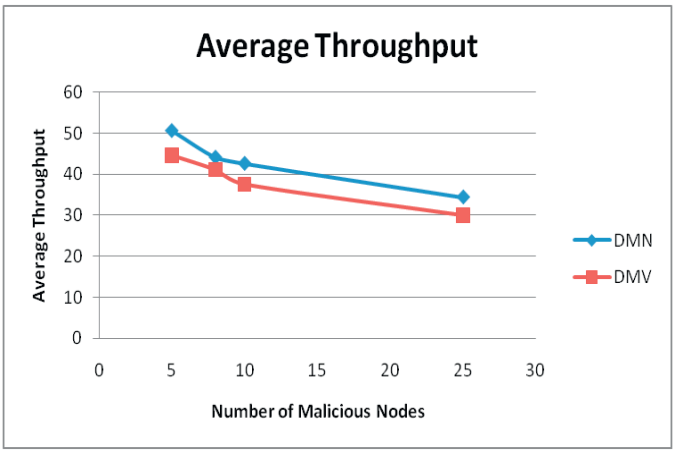


Figure1. Close to normal DMN and DMV performance research

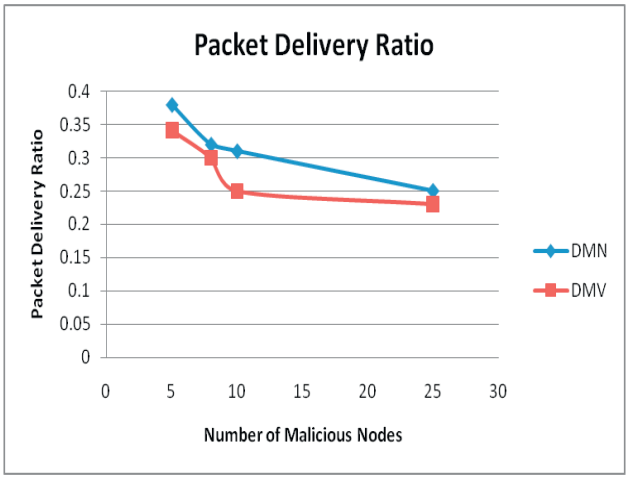
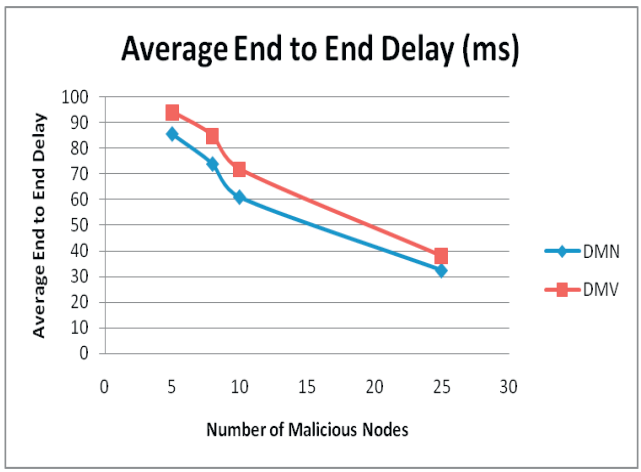


Figure 2. Near review of the DMN and DMV bundle transport ratio



Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

Figure 3. Relative review of normal beginning to complete DMN and DMV postponement

From the outcomes obtained, it is analyzed that DMN increases the likelihood of network execution of DMV by increasing the frequency with which verifier hubs are identified. It clearly and unequivocally demonstrates the higher levels of Normal Throughput, Parcel Conveyance Proportion, and Postponement Time vs the DMV, as far as what the preferred outcomes were.

6.Conclusion

We created DMN, a novel calculation for distinguishing mischievous activities and malignant vehicular hubs in VANETs (Discovery of Pernicious Hubs in VANETs). The DMN calculation is intended to seclude strangely acting hubs while as yet expanding network execution. DMN enhances the arrangement of verifier hubs, which play out the reason for checking hub conduct . DMN improves the DMV calculation, which chooses all hubs with a doubt esteem not exactly the vehicle to be checked as verifiers. Our proposed DMN calculation improved it by considering three boundaries when choosing fitting verifiers: burden, distance, and doubt esteem. These boundaries are utilized to decide a choice worth, which is then contrasted with the verifier determination limit. Picking the best verifiers improves the organization thus. By expanding network usage, this improves network unwavering quality. The reproduction results show that DMN has a higher throughput, a superior parcel transmission proportion, and a lower start to finish inertness than the DMV

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

calculation tried in various situations in our reenactment setting. A vindictive hub security system could be applied to the proposed work. In the event that the proposed approach is applied continuously, it is simpler to gauge and test its exhibition under certifiable things.

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.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication：Online Open Access
Vol: 40 Issue: 06-2021
DOI 10.17605/OSF.IO/9X8CY

[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 9$1(7¶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.