A Honeypot Scheme to Detect Selfish Vehicles in Vehicular Ad-hoc Network

Priya Patel[1,1], Rutvij Jhaveri[1],

[1] Department of Computer Engineering,
SVM Institute of Technology,
Bharuch 392-001, Gujarat, India
{piyubhandari11@gmail.com, rhj_svmit@yahoo.com}

Abstract. Vehicular Ad hoc network (VANET) has been emerged as a prominent technology for intelligent transportation systems. A VANET consists of a number of vehicles equipped together for communication on road side. VANETs are used to fulfil many requirements such as drivers' safety, data transformation and traffic control, and so on. In VANET, each vehicle behaves independently and as a result, some vehicles might behave selfishly to save their resources. This issue can induce network latency, network break down, security breach and other issues. In this paper, we address this issue by proposing a honeypot detection approach which endeavors to mitigate selfish vehicles from the network. For experimental results, proposed scheme is incorporated with AODV protocol. We present the behavior of selfish vehicles based on energy constraints. Simulation results under various network parameters depict that the proposed approach provide more robust and secured routing among the vehicles in VANETs.

Keywords: Vehicular ad hoc networks, selfishness, Bait mechanism, AODV

1 Introduction

Vehicular Ad hoc Network defined as number of vehicles connected together wirelessly and established the network on road route to communicate with each other for different purpose. VANET is another sort of specially appointed network that is described by its exceptionally mobile topology [1]. VANET is more preferable network because of its special features like unconstrained deployment, infrastructure less network, distributed nature, self-arranging nature and geographical independence [2]. These nature make it's more utilizable in many application areas like road safety, rout planning assistance, tolling, traffic management and many more [3]. VANET can be categorized in three diverse types based on its communication style: i) Vehicle to vehicle (V2V) communication, ii) Vehicle to road infrastructure (V2I) communication and iii) Vehicle to broadband cloud (V2B) communication [4].

In VANET, the routing protocols are categorized in various types: Topology based routing protocol – in which existing link used for packet forwarding, Position based

routing protocol - in which, the forwarding choice by node is essentially made in view of the position of the packet's destination and node's one-hop neighbors, Cluster based routing protocol – used for clustering network, in which routing decision taken by cluster head, Geo-cast routing protocol - these protocols are utilized for sending message to vehicle which locate in predefined geographical region, and Broadcast routing protocol- Broadcast routing is much of the time utilized as a part of VANET for sharing activity, climate and crisis, street conditions among vehicles and conveying notices and announcements [4-5].

There are many terms which effect network like energy efficiency, number of vehicles, resources and security of the data transmission over network. In VANET, each vehicles behave independently, from that some vehicles behave selfishly by dropping packets during routing or transmission to full feel their malicious purpose. The selfish vehicles use the network without pay back for the usage of network [7]. So result of these malicious activates on network QoS become low in terms of network breakage, latency occurred, low transmission rate, less security, energy constraints etc.

To address the selfishness problem in the network, many researchers develop the different techniques and mechanisms. There are various techniques developed to solve different types of selfish vehicles like, energy based, speed based, memory based and so on. Here in our work we proposed a solution for the energy based selfish vehicle. Here we developed the selfish vehicles which aim to save its energy. We designed the selfish vehicle which drop the packets when it's remaining energy less than 50% of total energy.

For prevention of the network from the selfish environment, numerous strategies were produced in past years by numerous researchers. Trust based approach, watchdog model based, Reputation based approach and many more. These mechanism provide security but in some scenario, some of technique increase overhead, and in trust based approach more memory required. So here we proposed honeypot mechanism based selfish vehicle detection scheme named as honeypot selfishness detection scheme (HPSD). This HPSD use honeypot mechanism to detect selfish vehicles when vehicle noticed as suspicious vehicles by its activities. After that it add into the suspicious list, bait RREQ unicast to that suspicious vehicle if it drop the bait packet then it's mentioned as selfish vehicle. And discard it from the network.

The rest of the paper is describe as: Section 2 describes selfishness in which types of selfish vehicles and its prevention techniques mentioned, Section 3 presents related work of different mechanisms developed by numerous researchers in past years to solve selfishness problem, section 4 represent existing and proposed approach for mitigating selfish vehicles from the network, section 5 represent simulation results and finally, in section 6 conclusion is mentioned.

2 Selfishness

2.1 Selfish Vehicles

In VANET, the vehicles which does not want to participate, drop the packet during routing and transmission process known as Selfish vehicles. They generally expect to expand their own benefit, bringing about undesirable postponements in the message conveyance and expansion the network inertness, which thus influences the whole execution of the network. The main goal behind this types of behavior of selfish vehicles is to save their resources like battery power, memory, CPU utilization, and bandwidth. Another reason behind these types of behavior might be fear of getting harmful data or information from neighbor vehicles. Energy is the critical parameter for vehicular ad hoc network because of low assets, these selfish vehicles may carry on as ravenous and they take the information from other vehicles when they require however they abstain from sending it to other vehicles in the network [8]. Based on the vehicles' different behavior, selfish vehicles categorized in three types [9]: Type 1: vehicles which does not participate in routing, Type 2: No response to HELLO message, Type 3: Drop the data packet.

2.2 Selfish Vehicles in AODV based VANET

In Fig. 1(a) VANET scenario shown, in which A vehicle is act as a source vehicle and G vehicle act as a destination vehicle. Now A vehicle want to communicate with vehicle G. For that A vehicle broadcast RREQ packet to its all neighbor vehicle to know whether G vehicle is its neighbor node or not (refer Fig. 1(b)).

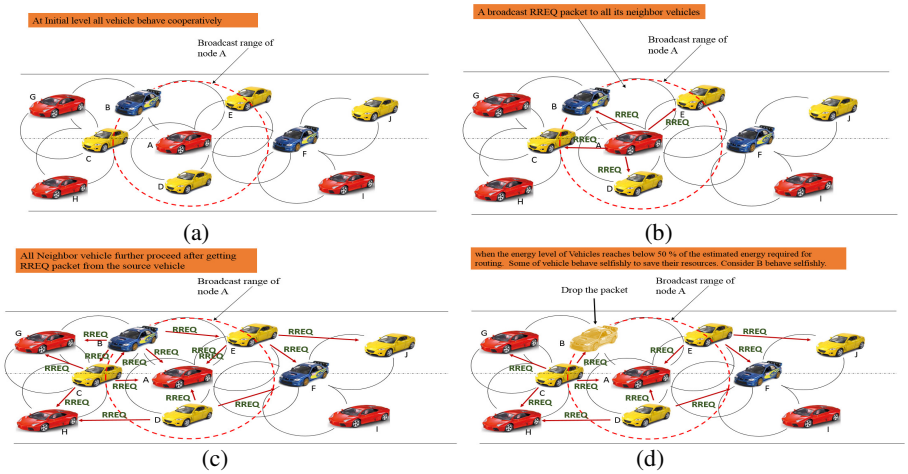


Fig. 1: Route discovery in VANET. a. Initial scenario b. route discovery c. route discovery in cooperative environment d. route discovery in selfish environment

Now in cooperative environment all vehicles check the RREQ packet and compare destination id with its own. If destination id matches then it forward RREP packet to source node and communicate with it directly. But if destination vehicle Id not match with its own Id then it further broadcast RREQ packet to its neighbor vehicle until it gets destination (as shown in Fig. 1(c)). Now as shown in Fig. 1(d), if selfish vehicle is present in network, it simply drop the packet and do not further broadcast RREQ packets to its neighbor. Here in Fig. 1(d) shows that vehicle B is behave selfishly and drop the RREQ packet during routing from source vehicle A to destination vehicle G.

2.3 Model of selfish vehicles based on energy constraint

In our work, we used to implement energy based selfish vehicles, i.e. its purpose to save its remaining energy. Here we take Type 1 selfish vehicles, which does not want to participate in the routing process. For that it drop the RREQ packet broadcasted from its neighbor node.

Action of Selfish vehicles after receiving RREQ message
IF(Energy of the Vehicle less than 50%)
Selfish Vehicle drop the packet
ELSE IF Vehicle check the Destination vehicle ID
Destination Vehicle ID match with vehicle ID
unicast RREP message to the Source Vehicle
ELSE
Further broadcast RREQ to its neighbor Vehicle
END IF

Fig. 2. Model for selfish vehicle

As shown in Fig. 2 we implemented the selfish vehicles, which behave selfishly i.e. drop the RREQ packet when it's remaining energy is less than 50% of total energy. Here as shown in above model, if energy level of selfish vehicles is less than 50%, then its drop the packet unless it's behave cooperatively. If vehicle is cooperative then its first check destination Id of the RREQ packet with its own, if destination Id matched then it unicast RREP packet to the source or current source and communicate with its. And if Destination id is not matched with its id then it further broadcast the RREQ packets to its neighbor to reached destination.

2.4 Techniques for Selfish vehicles detection

There are mainly three techniques developed for detecting selfish vehicles from the network.

Credit Based Schemes

In proposed scheme, each node have to pay some money to use services of the network. This money is like credit which is given to the intermediate nodes [11]. Those nodes which provides the services earn the credit and the in other hand those

nodes which uses the services have to pay the credit for that. The main agenda of this proposed scheme is to motivate the nodes for reliably behave in the network during transmission [12].

Reputation Based Schemes

In Reputation based schemes, matrix of reputation of nodes established based on the each nodes' behavior which is observed by its neighbor in the network. This reputation matrix is used to evaluate whether node is trustworthy or not. This information is then propagated throughout the network so that the detected misbehaving node can be removed from the network [11].

Acknowledgment Based Schemes

Proposed scheme is purely based on the reception of acknowledgement to verify the message is forwarded from the sender or not. In this types of technique monitoring of RREQ and RREP packet from neighbor nodes used to detect selfish nodes from the network. Furthermore, there are three types of module integrated: (i) Reputation module, (ii) Route discover module and (iii) Audit module [11].

3 Related Work

Selfishness of the vehicles is real issue of the VANET which influence the system's quality furthermore throughput. In later past year, numerous analysts have built up various methodologies to overcome issue of selfishness in different types of network.

Omar *et al. [1]* proposed two phase based Quality of service optimized link state routing (QoS-OLSR) protocol which was used to detect selfish vehicle from the clustered network. Here selfish vehicle behave selfish during cluster formation by providing fake information regarding to vehicle's speed. Incentive was used to detect selfish vehicle during cluster formation. But still selfish vehicle have benefits to behave selfishly after cluster formed. To solve this problem, in second phase cooperative watchdog model based Dempster-Shafer model used. Younes *et al. [8]* proposed a Secure Congestion contrOL (SCOOL) protocol. This protocol provides integrity and authenticity of transmitted data and also provide to preserve the privacy of the cooperative vehicles and drivers. Yang *et al. [13]* Proposed dynamic three – layer Reputation Evidence Decision System (REDS). In which, to discriminate selfish vehicles, Dempster-Shafer evidence integration mechanism used. This proposed scheme provide rapid solution for selfish node detection. Song *et al. [14]* proposed privacy-preserving distance based incentive scheme to detect location privacy and behavior of selfish nodes. Zhou *et al. [15]* proposed trust based approach named security authentication method. Here two types of trust evaluation technique used. First was direct trust, in which the security vector model was set up taking into account the security practices of the new vehicle node. And second was indirect trust, in which the trust degree is computed in light of the proposal trust vectors from the vehicle nodes in the system. Khan *et al. [16]* proposed DMN – Detection of Malicious Nodes is improved version of DMV algorithm in terms of selection of selfish nodes. Jesudoss *et al. [17]* proposed Payment Punishment Scheme (PPS) which not only detect selfish vehicles but also used to encourage selfish vehicles cooperatively after cluster formation. Here watchdog model used to monitor the

vehicles and modified Extended Dempster–Shafer model used to discourage the vehicle from selfish behavior.

4 Existing and Proposed Approach

4.1 Existing Approach

During creation of a path, source vehicle checks its routing table first. Then if the destination vehicle is not present than it broadcast the RREQ message to all neighbor vehicles. The cooperative neighbor vehicle will again rebroadcast it to their one hop neighbor vehicles and this process continues until it reaches destination vehicle [10]. Meanwhile source vehicle is also a one hop neighbor node of each of these nodes so it will receive the same. So each time vehicle monitor its neighbor vehicles' character based on receiving back RREQ packet from neighbors. If it has not received the same RREQ from one of its neighbor vehicles within a prefixed timeout then that node will be marked as potential misbehaving vehicle. This process continues repeatedly. For each potential misbehaving node, a threshold value is maintained. If the number of times a vehicle is marked as a potential misbehaving node beats this threshold limit, then that vehicle will be declared as selfish vehicle and this information will be sent to all other vehicles of the network [10]. After detecting selfish vehicles in the network, new path established through game theory, which help to find shortest path from the source to destination.

4.2 Proposed Approach

To improve the existing approach here for detection of selfish vehicles Bait method used in which whenever any vehicle drop the packet, Bait mechanism used for detection of selfish vehicles.

During creation of a path, source vehicle checks its routing table first. Then if the destination vehicle is not present than it broadcast the RREQ message to all neighbor vehicles. The cooperative neighbor vehicle will again rebroadcast it to their one hop neighbor vehicles and this process continues until it reaches destination vehicle. Meanwhile source vehicle is also a one hop neighbor node of each of these nodes so it will receive the same. So each time vehicle monitor its neighbor vehicles' character based on receiving back RREQ packet from neighbors. If it has not received the same RREQ from one of its neighbor nodes within a prefixed timeout then current source node send the Bait RREQ to its suspicious neighbor. If suspicious vehicle drop that Bait RREQ packet then that vehicle will be marked as selfish Vehicle otherwise if it broadcast that Bait RREQ packet then it will be marked as cooperative Vehicle. After that all path entry related to that selfish vehicle will be deleted and route hand off process done for new path. Among all possibility shortest path will be select for further process.

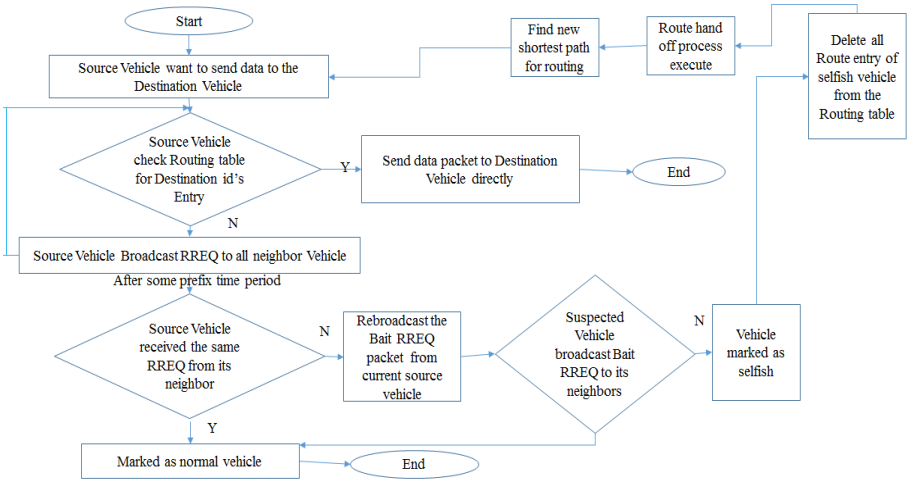


Fig. 3: Flowchart of proposed approach

5 Simulation Results

The simulation is carried out on NS-2 and SUMO simulator. Scenario for the VANET generated using OSM. Here simulation is carried out in 1000x1000 m area of simulator, where AODV, SVAODV and HPAODV were executed. The performance of these three routing protocol measured in four different metrices: PDR, Normalized Routing Overhead, End to End Delay and Average Consumed Energy. The major simulation parameters are listed in below Table 1. Furthermore VANET scenario of the network in SUMO shown in Fig. 4.

Table 1: Simulation Parameters

Parameters	**Value**	**Parameters**	**Value**
Simulator	NS 2.34	**Pause Time**	5 sec
Routing Protocol	AODV,SVAODV, HPAODV	**Maximum Speed**	5,10,15,20,25 m/sec
Scenario Size	1000 x 1000 m	**Initial Energy**	300 J
Number of Vehicles	20,40,50,60,80,100	**Transmit Power**	1.65 W
Selfish Vehicles	0,2,4,6,8	**Receive Power**	1.4 W
Simulation Time	240 Sec	**Idle Power**	1.15 W
Traffic Types	Constant Bit Rate (CBR)/ UDP	**Sleep Power**	0.045 W
Number of Connection	5	**Transition Power**	2.3 W
Packet Rate	4 packets/sec	**Transition Time**	800 µs

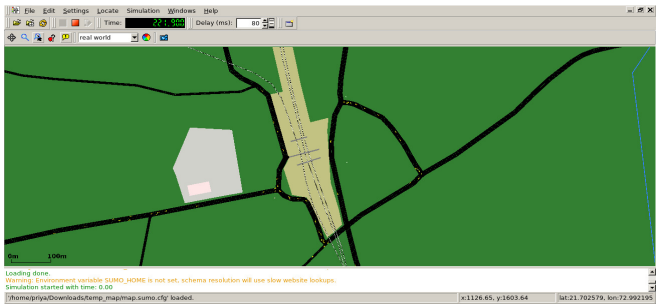
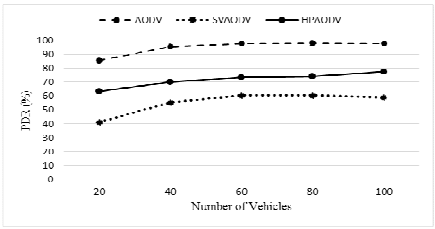


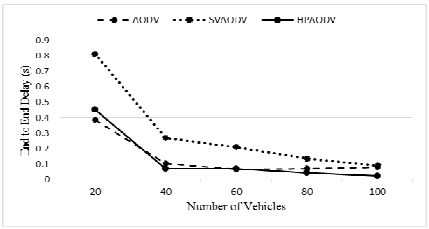
Fig. 4: VANET scenario

5.1 Test 1: Varying number of vehicles

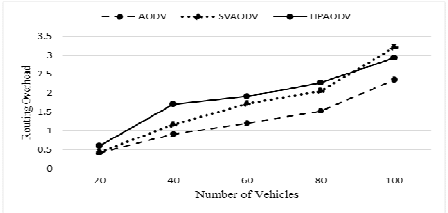
As shown in Fig. 5.1 (a), in the absence of selfish vehicles, AODV gives more than 98% PDR for all network sizes. When in presence of selfish vehicles PDR decrease up to 50%. When proposed approach applied on the system, it improve result in terms of PDR up to 20-25 % then selfish environment. Furthermore, proposed approach reduce up to 30-50 % End to End Delay during transmission. Because proposed approach take quick action after getting suspicious vehicle in the network, so it provide the robust solution (As shown in Fig. 5.1(b)). Despite of this beneficial results, proposed scheme increased Normalized Routing Overhead (Refer Fig. 5.1 (c)). Which is drawback of the proposed work. As shown in Fig. 5.1(d), Energy consumption became low in selfish environment.



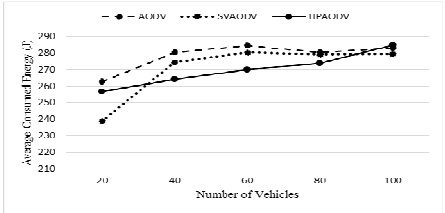
(a)



(b)



(c)

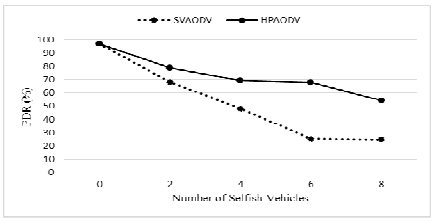


(d)

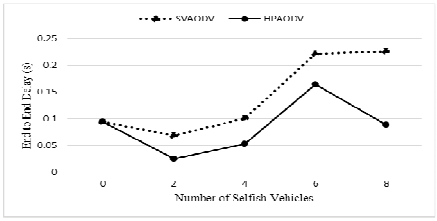
Fig. 5.1 (a) PDR (b) End to End Delay (c) Normalized Routing Overhead (d) Average Consumed Energy - when number of vehicles vary

5.2 Test 2: Varying number of selfish vehicles

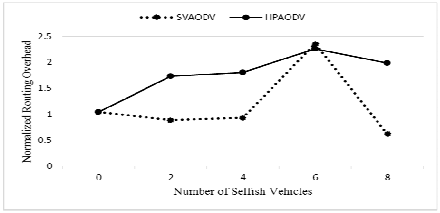
As shown in Fig. 5.2 (a ,b ,c ,d), as per selfish vehicles were increased PDR, End to End Delay, Normalized Routing Overhead and Average Consumed Energy were decrease, increase, increase and decrease respectively. In this test scenario, 0 number of selfish vehicles present normal AODV protocol scenario. When proposed honey pot approach applied, it increase the PDR up to 30%, decrease end to end delay up to 20%. During increasing of selfish vehicles in the network, the PDR of the HPAODV protocol decreased. In terms of Normalized routing overhead, proposed approach not provide better result. Energy consumption of proposed approach changes with respect to number of selfish vehicles increase in the network.



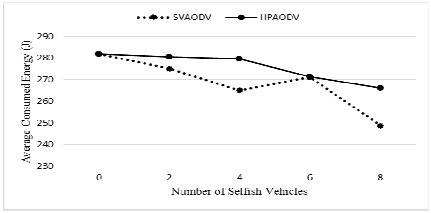
(a)



(b)



(c)



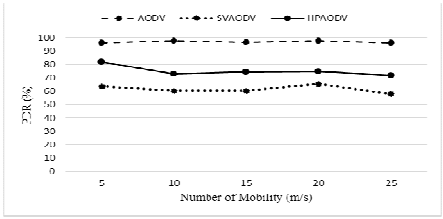
(d)

Fig. 5.2 (a) PDR (b) End to End Delay (c) Normalized Routing Overhead (d) Average Consumed Energy - when number of selfish vehicles vary

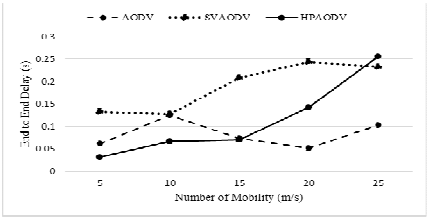
5.3 Test 3: Varying number of mobility

As shown in Fig. 5.3(a), in the absence of selfish vehicles, AODV gives more than 98% PDR for all network sizes. When in presence of selfish vehicles PDR decrease up to 30% - 40%. Now when proposed scheme applied it improve the result of packet delivery ratio up to 20-25% efficiently. As mobility increased, drastic increment occurred in terms of end to end delay in network. Now when proposed approach apply on the network it able to reduce unexpected delay of the network. As shown in Fig. 5.3 (b), Routing overhead increased in both scenario (i.e. in normal AODV and in SVAODV). Here proposed approach fail to reduce the routing overhead of the network. Moreover, when proposed approach applied on the network it able to reduce

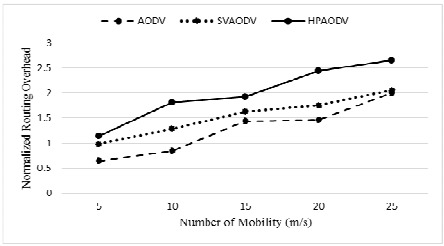
average energy consumption by vehicles, which make it more reliable in terms of lifetime of the network.



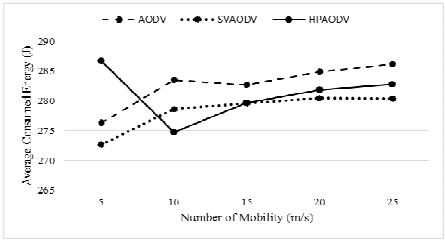
(a)



(b)



(c)



(d)

Fig. 5.3 (a) PDR (b) End to End Delay (c) Normalized Routing Overhead (d) Average Consumed Energy - when mobility vary

5.4 Comparison of Existing approach with proposed approach

In existing approach, detection of selfish vehicle done by comparing the threshold value of potentially misbehaving vehicle with pre-defined threshold value. When in the proposed approach based on Bait detection scheme in which if vehicle drop the packet then current source vehicle send fake message packet to vehicle. If target vehicle response to that message than it consider as selfish node.

In existing scheme, after some amount of packet dropping behavior existing scheme take action. Where in proposed scheme at the time when packet dropping behavior recognized by the node, it take action to detect selfish vehicle.

Table 2. Comparison of proposed approach and proposed approach

Properties	Existing Approach	Proposed Approach
Detection Technique	Based on threshold value	Based on Bait mechanism
Accuracy of detection of selfish node	Less/ Average (Expected)	More
Processing Time for detection selfish node	More	Less
PDR	Less (Expected)	More

6 Conclusion

Vehicular Ad hoc Network has been an active research area in recent years due to its ubiquitous nature and need of intelligent transportation systems for developing smart cities. This is advantageous on one hand, while proves to be disadvantageous when selfish vehicles start misbehaving. Selfishness is a serious issue in VANET, which directly affects PDR of the network. To solve selfishness problem, here we introduced honeypot selfish vehicle detection scheme. Proposed scheme based on bait RREQ packet, which manipulate selfish vehicle to behave selfishly again so that it can be detected.

The simulation results show that performance of the AODV protocol in presence of selfish vehicles degrade performance up to 30-50% in terms of packet delivery rate. Furthermore, routing overhead and delay increase than that of normal AODV protocol. Due to the characteristics of selfish vehicles, the average consumed energy slips below to that of normal AODV where selfish vehicles are present in the network. Here proposed approach HPAODV is able to improve packet delivery ratio up to 30% and it also degrade the end to end delay. These make proposed approach more effective in terms of network lifetime. However due to proposed approach, overhead will be increased in the network because of multiple forwardness of fake request packets to detect selfish vehicles over the network. Here this is the drawback of proposed scheme, which can be taken as future work.

References

1. Wahab, Omar Abdel, Hadi Otrok, and Azzam Mourad. "A cooperative watchdog model based on Dempster–Shafer for detecting misbehaving vehicles." Computer Communications 41 (2014): 43-54.
2. Jhaveri, Rutvij H., and Narendra M. Patel. "A sequence number based bait detection scheme to thwart grayhole attack in mobile ad hoc networks."Wireless Networks 21, no. 8 (2015): 2781-2798.
3. Lipiński, Bartosz, Wojciech Mazurczyk, Krzysztof Szczypiorski, and Piotr Śmietanka. "Towards effective security framework for vehicular ad-hoc networks." Journal of Advances in Computer Networks 3, no. 2 (2015).
4. Liang, Wenshuang, Zhuorong Li, Hongyang Zhang, Shenling Wang, and Rongfang Bie. "Vehicular ad hoc networks: architectures, research issues, methodologies, challenges, and trends." International Journal of Distributed Sensor Networks (2014).
5. Andrey, Ostroukh Vladimirovich, and El hadi Hamrioui. "Comparative Study of Routing Protocols in Vehicular Ad-Hoc Networks (VANETS)." International Journal of Advanced Studies 4, no. 2 (2015): 9-14.
6. Altayeb, Marwa, and Imad Mahgoub. "A survey of vehicular ad hoc networks routing protocols." International Journal of Innovation and Applied Studies 3, no. 3 (2013): 829-846.
7. Helen, D., and D. Arivazhagan. "Applications, Advantages and Challenges of Ad Hoc Networks." JAIR 2, no. 8 (2014): 453-7.
8. Younes, Maram Bani, and Azzedine Boukerche. "Scool: A secure traffic congestion control protocol for VANETs." In Wireless Communications and Networking Conference (WCNC), 2015 IEEE, pp. 1960-1965. IEEE, 2015.

9. http://eprints.utm.my/33353/2/MahmoudAhmadSalemMFSKSM2012CHAP1.pdf
10. Das, Debjit, Koushik Majumder, and Anurag Dasgupta. "Selfish node detection and low cost data transmission in MANET using game theory."Procedia Computer Science 54 (2015): 92-101.
11. Agarwal, Dikshita, Rashmi Ranjan Rout, and Sadam Ravichandra. "Detection of node-misbehavior using overhearing and autonomous agents in wireless Ad-Hoc networks." In Applications and Innovations in Mobile Computing (AIMoC), 2015, pp. 152-157. IEEE, 2015.
12. Mittal, Sumit. "Identification Technique for All Passive Selfish Node Attacks In a Mobile Network." International Journal 3, no. 4 (2015).
13. Yang, Yang, Zhipeng Gao, Xuesong Qiu, Qian Liu, Yuwen Hao, and Jingchen Zheng. "A Hierarchical Reputation Evidence Decision System (REDS) in VANETs." International Journal of Distributed Sensor Networks 501 (2015): 341579.
14. Song, Jun, ChunJiao He, Fan Yang, and HuanGuo Zhang. "A privacy-preserving distance-based incentive scheme in opportunistic VANETs."Security and Communication Networks (2015).
15. Zhou, Ao, Jinglin Li, Qibo Sun, Cunqun Fan, Tao Lei, and Fangchun Yang. "A security authentication method based on trust evaluation in VANETs."EURASIP Journal on Wireless Communications and Networking 2015, no. 1 (2015): 1-8.
16. Khan, Uzma, Shikha Agrawal, and Sanjay Silakari. "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks." Procedia Computer Science46 (2015): 965-972.
17. Jesudoss, Auxeeliya, SV Kasmir Raja, and Ashraph Sulaiman. "Stimulating truth-telling and cooperation among nodes in VANETs through payment and punishment scheme." Ad Hoc Networks 24 (2015): 250-263.