A Perspective of Probabilistic Misbehavior Detection Scheme in Vehicular Ad-hoc Networks

M Arutselvan, T V Ananthan, G Sreeram

Abstract*: *Nowadays Vehicular Ad-hoc Networks fascinated lot of researchers to work on it in different perspectives, Such as Mobility Models, Routing Protocols, Security and so on.The exchange of safety information plays the key role in different real-time applications, such as alert function of safety travel and lane merging. In the absence of security, varieties of attacks are possible in VANET, such as dissemination of false warning communications and destruction of actual warning communications, thereby causing calamities. This emphasis security a major anxiety in such networks. This paper mainly concentrates on security aspects of Vehicular Ad-hoc Network.The main concern of this paper is to analyze the usefulness and proficiency of Probabilistic Misbehavior Detection Scheme in Vehicular Ad-hoc Networks. By implementing Probabilistic Misbehavior Detection Scheme in Vehicular Ad-hoc Network, malicious nodes in the network are identified and corrective actions made. Thus preventing the degradation of network and increasing its efficiency. This paper present the preliminary simulation results showing the usefulness and proficiency in graphical format.The performance of the proposed techniqueis compared with existing methods in terms of end-to-end delay, packet delivery, packet loss and throughput.

Index Terms*: *efficiency, malicious, probabilistic, performance, Vehicular Ad hoc Network.

I. INTRODUCTION

Current developments in short-range wireless technologies have empowered a new wealth of networking possibilities for user devices. In particular, ad hoc networks have appeared as one of the most researched areas in the networking community over the last few years. An ad-hoc network consists of a set of nodes prepared with wireless interfaces, which are able to communicate among themselves in the absence of any kind of network infrastructure. One of the most salient features of ad hoc networks is the concept of wireless hop-to-hop communications Unlike old-fashioned wireless networks, mobile nodes are allowed to send messages to destinations that are not within the sender's radio range. When the destination node is several hops away, in-between ad hoc nodes act as relays to forward data packets to their intended destinations. Therefore, nodes need to use a routing protocol to discover paths to deliver data messages from source to destinations. In general, ad hoc nodes can be portable, which makes the design of routing protocols a very challenging task. In recent years the outburst in the interest leading towards VANET, research community and automobile community have started to work towards an efficient and secured inter vehicular communication [1], [2], [4]. Researchers are striving towards providing an intelligent transportation system with all inbuilt and external comforts towards their passengers [5], [7], [13].The prominenceimpact of VANETs established by the rapid proliferation of associations involving car manufacturers, various government agencies, and academia. VANET provides wireless communication between moving vehicles and other vehicles either moving or hauled, they provide wireless interface between vehicles and fixed roadside equipment [1]. Here each vehicle furnished with several accurate sensors, to collect the information of neighboring.

In VANET vehicles act as mobile nodes and these nodes can form network with vehicles, which come in the range of each other [13]. The original inspiration for VANET was to encourage traffic safety; recently it has become increasingly evident that VANETs open new vistas for Internet access and the fast-growing mobile entertainment industries.VANET communication can help in avoiding critical situations like traffic jams, unseen obstacles and accidents. Hence, they assist the customers to coordinate and communicate in order to provide a secured navigation, with intelligence, for ease of humanity [15].VANETs differ from the existing MANETs only by few characteristics [9]. MANETs considered being slow in speed in comparison to VANET, making VANETs highly challenging. Hence successful delivery of data packets in VANET are highly import (to reach from source node to the destination node) under such a high speed and frequent change in topology [2]. The frequent change in topology has made VANET less reliable and more unsafe for data communication compared to MANET [8]. Hence researchers throughout the globe made remarkable research in the field of VANET to provide each user with secured and efficient data communication as per the given situation and criticality.

Due to high mobility of vehicles in VANET, the distribution of vehicles (nodes) within the considered scenario changes rapidly and unexpectedly. Due to high mobility, VANET experiences frequent link breakages [10].

Revised Manuscript Received on April 07, 2019.

M Arutselvan, Department of CSE & IT, Dr. M G R Educational and Research Institute, Chennai, T N, India.

T V Ananthan, Department of CSE & IT, Dr. M G R Educational and Research Institute, Chennai, T N, India.

G Sreeram, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, A.P, India.

Unexpected and misleading information in VANET can lead to a heavy traffic jam or a critical collision between vehicles, which can be life threatening. Such altered message can be generated from the source vehicle or any member (in hop by hop communication) vehicle, routing the information from the source node to the destination vehicle.Packet dropping or not forwarding the packet by selfish or malicious vehicle will also severely degrade the network performance.

The rest of this paper is structured as follows. Related works are presented in Section 2, whereas problem methodology and system models are detailed in Section 3. Section 4 elaborates on our proposed technique. Section 5 presents the result analysis and performance evaluation. Finally, Section 6 concludes by restating the contributions of this paper.

II. RELATED WORKS

Yao-Hua Ho, Chun-Han Lin and Ling-Jyh Chen [12] have presented an On-demand Misbehavior Detection technique for vehicle-to-vehicle communication. In their technique, they adapted two location-based routing protocols such as "Contention-Based Forwarding and Connectionless Approach for streets".

Bitam et al [14] have presented a hybrid Bee swarm routing (HyBR) protocolbased on the continuous learning paradigm. The above-mentioned protocol syndicatesthe features of topology routing with those of geographic routing. HyBR is a unicast and multipath routing protocol that guarantees road safety services by transmitting packets with minimum delays and high packet delivery.Sharing the integrateddata with road safety service in real time is the most important necessities in the routing process for providingthe information passengers need to help them make safe decisions. This protocol united the properties of geographic routing with those of topology routing.

Nasir et al. [15] effectively proposed the necessity for the vigorous VANET networks that were largely dependents on safety and secrecy traits. The multifarious challenges encountered by the VANET were appropriately addressed in their investigation. In addition, they also deliberated on a set of feasible solutions offered for facing the grave challenges and issues and the solutions were effectively criticized.

Gaur et al. [16] were instrumental in detailing fact that the VANETs were likely to become the networking platform that would assist the forthcoming vehicular applications. They effectively investigated the vital factors in ascertaining the networking structure above which the potential vehicular Applications employed. A reactive investigation Endeavour was the need of the hour for translating the concept of VANETs in to a reality in the days to come.

Chim et al [17] presented a navigation mechanism for gathering online road information by a VANET, which lets the drivers in the direction of the required destination in the real time method as well as in the distributed format. The driver privacywas guaranteed that is attained by the queries made by the destination and those who offers the query that cannot be connected to any of the nodes, which includes even the authenticated nodes. Attainment of the above method by the use of an unsigned recordwas unsalable due to the un-authentication problems.

Zhong et al. [18] have proposed a "conditional privacy-preserving and authentication scheme for secure service provision". The security analysis is not only gratifies the security acquirements such as message authentication, non-repudiation, unlink ability, and replay resistance. This scheme can enforce non-forgery of messages under the adaptive chosen message attack in the random oracle model. This model showcasedmore efficient in terms of computation cost and communication overhead, which makes it more suitable for deployment in VANET services and applications. This scheme satisfied the security requirements andoptimized the calculation process of signature generation and verification. Hu et al. [19] have introduced a "reliable trust-based platoon service recommendation scheme (REPLACE) to avoid badly-behaved platoon head vehicles". The design on reputation system to the platoon head vehicles for collecting and modeling their user vehicle's feedbacks. Then the design was made for an iterative filtering algorithm to deal with the untruthful feedbacks from user vehicles. The high changing aspects ensure the real-time update of feedbacks. The storage of feedbacks and computation of reputation scores enabled by hybrid architecture vehicles, RSUs, server and trust authority. The malicious vehicles intentionally manipulatedto provide fake feedbacks with each other. Cui et al. [20] have proposed the "secure privacy-preserving authentication scheme with Cuckoo filter (SPACF)", is based on software without relying on any special hardware. The Cuckoo Filter and the binary search methods used to achieves higher success rate in the batch verification phase. It is satisfied therequirement for message authentication, existential un-forge-ability of underlying signatureagainst adaptively chosen-message attack proved under elliptic curve discrete logarithm problem in the random oracle model. However, the computation power of a SPACF is not strong enough to handle allshort time verifications, especially in heavy traffic density places.

Wazid et al. [21] have presented a "lightweight authentication and key agreement protocol based on one-way hash functions and bitwise XOR operations".The generated information in the memory of roadside units are stored and deployed on different roadsides. In the memory of an onboard unit of a vehicle, the required information is stored so that it can be used for the authentication process later.The security analysis depictedthe security against various known attacks, and provided the additional functionality features, such as "efficient dynamic RSU addition phase, mutual authentication, vehicles and RSUs anonymity property, and un-traceability property".

III. PROPOSED METHODOLOGY

Zhaoyu Gao et al [22] have proposed a probabilistic misbehavior scheme for detecting malicious nodes in Delay Tolerant Network and consists of two phases are routing evidence generation phase and auditing phase. This scheme is based on Inspection game and used game theoretical analysis to overcome the drawback of network traffic overload.

As of Inspection game theory, the trusted authority in the delay tolerant network invokes the misbehavior detection on certain probability rather than periodical invocation for a particular node.

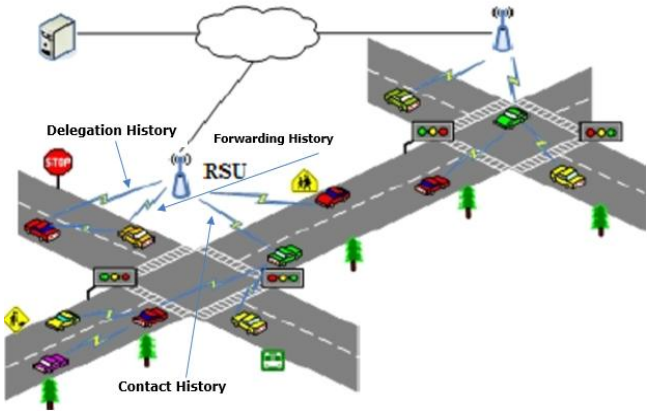

Figure 1: System Model

In Zhaoyu Gao et al [22]the Opportunistic Networking Environment Simulator is used for simulating this model and in that, First Contact Routing Protocol is used as the routing agent of the their technique. In this simulation, Packet Loss Rate is used as the indicator of misbehavior level of the malicious node. The parameters used are Detection Rate, False Detection Rate and Transmission Overhead Rate. In recent days, the foremost challenge in Vehicular Ad-hoc Network is its security. For providing the proper and efficient security, the methodology should pursue the security constraints for instance integrity, confidentiality, privacy, non-repudiation and authentication to shield against attackers and malicious vehicular nodes. The several attacks, such as instance black hole, Sybil, Denial-of-Service (DoS), Timing, Illusion etc. that are not only involve the privacy of drivers and vehicles but also compromise traffic safety and can direct to thrashing of life. The following statements points out the important notion of Probabilistic Misbehavior Detection Scheme in VANET:

1. We assume that the RSU in the VANET acts as Trusted Authority and it is responsible for invoking the Misbehavior Detection Algorithm on the particular Node in the network.
2. The Malicious Node detection is performed by using Modified Probabilistic Misbehavior Detection Algorithm.
3. Finally, the performance of PMDSVis compared with existing techniques in terms of detection rate, throughput and packet delivery ratio.

IV. PROBABILISTIC MISBEHAVIOR DETECTION SCHEME

In this section, we discuss about the detailed working function and mathematical model of proposed technique.

PMDSV Algorithm

The introduction of reputation system in the Inspection game will greatly reduce the transmission overhead in the network, which is incurred by triggering the misbehavior detection algorithm for every node in the network. A vehicle or node in the network at any point of time should have the reputation value r and roadside unit (RSU) generates a random detection probability and compares the reputation value of the detecting node with threshold value. If the reputation value of the detecting node is less than the threshold value and the random probability is less than the threshold detection probability, then RSU triggers the misbehavior detection algorithm. Otherwise, the reputation value of the detecting node is increased.

The working function of probabilistic misbehavior detection scheme is given in below algorithm.

Algorithm: PMDSV in VANET

```
1  Begin
2     Extract vehicles in network at T time period
3     Initialize the number of vehicles numVehicles
4     For each vehicle j do
5        Generate a random number randNum_j from 1 to
          10^numVehicles -1
6  if randNum_j/10^numVehicles < p_d and r_j < t_r then
7        ask all vehicles (including vehicle j) to provide
         evidence about vehicle j
8          if judge(vehicle j)==1 then
9             pay vehicle j the compensation c_p
10            increase the reputation value r_j of vehicle j
11         else
12            give a punishment p_t to vehicle j
13            decrease the reputation value r_j of vehicle j
14         end if
15       else
16         pay vehicle j the compensation c_p
17         increase the reputation value r_j of vehicle j
18       end if
19      if r_j < t_r then
20          Remove vehicle j from routing list and add it
          in blacklist
21          broadcast blacklist in the network
22 end for
23 end
```

According to the probability property, the value of p_d should not be greater than 1 which defines the upperbound of detection probability. The nodes considered malicious and are detected if itsdetection probability is one. The intervention of reputationsystem in PMDS enhance the efficiency of malicious node detection.Furthermore, the transmission error of a node with reputation r = 1could be tolerated by the reputation system.The main concern here is alower reputation node will increase its inspectionprobability as well as a decrease in its payoff.

V. RESULT AND ANALYSIS

In this section, we analyze the performance of proposed PMDSV technique with two testing scenarios: with/without malicious vehicles and comparison with PMDS. The proposed PMDSV technique is implemented on VANET simulator with JAVA platform. Here simulated a VANET composed of 100 nodes in fixed network size as 500×500 m^2 andthe selected traffic model is constant bit rate (CBR).In practice, anynode in the network can transmit at any time at a constant rate. The average speed of each vehicle is 40kmph and the maximum speed is 50kmph. The transmission packet size is 1400 bytes. We use the A* routing protocol for further routing between source-destination. The simulation will take 120 seconds of simulation time. The parameters of simulation environment are illustrates in Table 1.

Table 1 Simulation parameters

Parameter	Value
Network size	500 × 500 m^2
Number of vehicles	20, 40, 60, 80, 100
Number of malicious nodes	1, 2, 3, 4,5
Average speed	40kmph
Maximum speed	50kmph
Packet size	1400 bytes
Traffic model	CBR
Routing protocol	A*
Simulation time	120 seconds

The performance of PMDSV is compared with existing PMDS technique in terms of minimum detection time, number of detection nodes, delay, delivery ratio, drop ratio, and throughput. Fig. 2 illustrates the packet delivery ratio comparison of PMDS and PMDSV. Here, the values are calculated by varying the number of vehicles in the network.

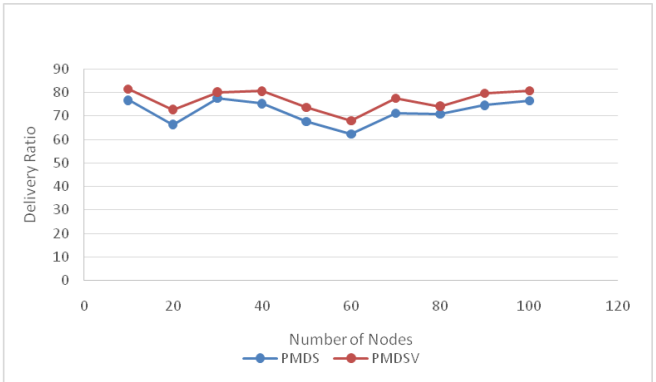

Figure 2. PDR comparison PDMS & PDMSV

Fig. 3 illustrates the end-to-end delay comparison of PMDS and PMDSV. As the graph implies that the delay increases as the number of malicious vehicles increases. But compared to PMDS, the PMDSV reduces the delay in the vehicular ad-hoc network by incorporating the reputation system.

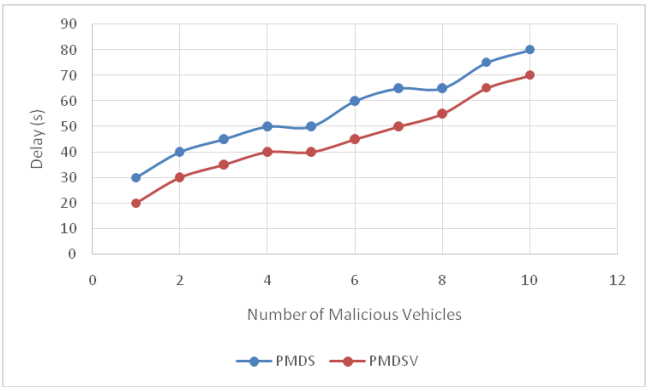

Figure 3. End-to-End Delay Comparison

Fig. 4 illustrates the detection probability of PMDS and PMDSV. By tuning to the proper detection probability, the PMDSV could almost detect all the malicious vehicles in the network.

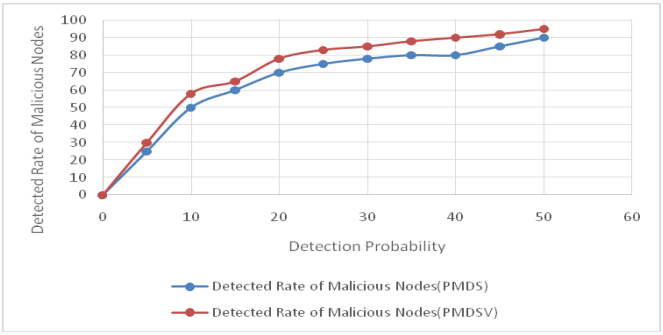

Figure 4. Detection Probability Comparison

VI. CONCLUSION

In this paper, we propose a probabilistic misbehavior detection scheme (PMDSV) for Vehicular Ad-hoc Networks, which could increase the network safety by identifying the misbehaving vehicles with reduced detection overhead. The implementation of reputation system in the misbehavior detection system helps in greatly increasing the detection efficiency. Finally, the performance of PMDSV is compared with PMDS in terms of Packet Delivery Ratio, End-to-End Delay and Detection Probability.

REFERENCES

1. V. Lakshmi Praba and A. Ranichitra, "Detecting Malicious Vehicle in a VANET scenario by incorporating security in AODV Protocol", ICTACT Journal on Communication Technology, Vol. 3, No. 3, 2012.
2. YinghuiGuo, et al. "A Misbehavior Detection System for Vehicular Delay Tolerant Networks", GI-Jahrestagung, pp. 1871-1877, 2012.
3. Uzma khan, et al. "Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks", Procedia Computer Science 46, pp. 965-972, 2015.
4. Uzma khan, et al. "A Detailed Survey on Misbehavior Node Detection Techniques in Vehicular Ad Hoc Networks", Information Systems Design and Intelligent Applications, Springer India, pp.11-19, 2015.
5. A. Daeinabi, et al. "Detection of Malicious Vehicles (DMV) through monitoring in Vehicular Ad hoc Networks", Multimedia tools and applications, Vol. 66, No. 2, pp. 325-338, 2013.

6. Shefali Jain, et al. “Misbehavior Detection in VANET: A Survey”, Security, Privacy, Trust and Resource Management in Mobile and Wireless Communications, pp. 134, 2013.
7. M. Altayeb, and I. Mahgoub, “A Survey of Vehicular Ad-hoc Networks Routing Protocols”, International Journal of Innovation and Applied Studies, Vol.3, pp.829-846, 2013
8. S. Asoudeh, M. Mehrjoo, N. Balouchzahi and A. Bejarzahi, "Location service implementation in vehicular networks by nodes clustering in urban environments", Vehicular Communications, vol. 9, pp. 109-114, 2017.
9. X. Feng, C. Li, D. Chen and J. Tang, "A method for defensing against multi-source Sybil attacks in VANET", Peer-to-Peer Networking and Applications, vol. 10, no. 2, pp. 305-314, 2016.
10. B. Chang, Y. Liang and H. Yang, "Performance Analysis with Traffic Accident for Cooperative Active Safety Driving in VANET/ITS", Wireless Personal Communications, vol. 74, no. 2, pp. 731-755, 2013.
11. K. Abboud and W. Zhuang, "Stochastic Modeling of Single-Hop Cluster Stability in Vehicular Ad Hoc Networks", IEEE Transactions on Vehicular Technology, vol. 65, no. 1, pp. 226-240, 2016.
12. Yao-Hua Ho, Chun-Han Lin and Ling-Jyh Chen, “On-demand Misbehavior Detection technique for vehicle-to-vehicle communication”
13. C. Chen, I. Chang, C. Chang and Y. Wang, "A Secure Ambulance Communication Protocol for VANET", Wireless Personal Communications, vol. 73, no. 3, pp. 1187-1213, 2013.
14. S. Bitam, A. Mellouk and S. Zeadally, "HyBR: A Hybrid Bio-inspired Bee swarm Routing protocol for safety applications in Vehicular Ad hoc NETworks (VANETs)", Journal of Systems Architecture, vol. 59, no. 10, pp. 953-967, 2013.
15. Mostofa Kamal Nasir, A.S.M. Delowar Hossain, Md. Sazzad Hossain, Md. Mosaddik Hasan, Md. Belayet Ali, "Security Challenges And Implementation Mechanism For Vehicular Ad Hoc Network", international journal of scientific and technology research, vol. 2, no. 4, 2013.
16. Saurabh Kumar Gaur, S.K.Tyagi, Pushpender Singh, "VANET System for Vehicular SecurityApplications", international journal of soft computing and engineering, vol. 2, no. 6, 2013.
17. T. Chim, S. Yiu, L. Hui and V. Li, "VSPN: VANET-Based Secure and Privacy-Preserving Navigation", IEEE Transactions on Computers, vol. 63, no. 2, pp. 510-524, 2014.
18. H. Zhong, J. Wen, J. Cui and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET", Tsinghua Science and Technology, vol. 21, no. 6, pp. 620-629, 2016.
19. H. Hu, R. Lu, Z. Zhang and J. Shao, "REPLACE: A Reliable Trust-Based Platoon Service Recommendation Scheme in VANET", IEEE Transactions on Vehicular Technology, vol. 66, no. 2, pp. 1786-1797, 2017.
20. J. Cui, J. Zhang, H. Zhong and Y. Xu, "SPACF: A Secure Privacy-Preserving Authentication Scheme for VANET With Cuckoo Filter", IEEE Transactions on Vehicular Technology, vol. 66, no. 11, pp. 10283-10295, 2017.
21. M. Wazid, A. Das, N. Kumar, V. Odelu, A. Goutham Reddy, K. Park and Y. Park, "Design of Lightweight Authentication and Key Agreement Protocol for Vehicular Ad Hoc Networks", IEEE Access, vol. 5, pp. 14966-14980, 2017.
22. Z. Gao, H. Zhu, S. Du, C. Xiao and R. Lu, "PMDS: A probabilistic misbehavior detection scheme in DTN," 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, 2012, pp. 4970-4974.