International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 08 | Aug -2017 www.irjet.net p-ISSN: 2395-0072

THE NEW ROUTE DISCOVERY TECHNIQUE FOR SECURE MESSAGE DELIVERY IN VEHICULAR ADHOC NETWORK (VANET) USING DRI TABLE APPROACH

Ramandeep Kaur[1], Er. Rupinderpal Singh[2]

[1]M.Tech Student, Computer Science, Global Institute of Management & Emerging Technologies, PTU, Punjab
[2]HOD, Computer Science, Global Institute of Management & Emerging Technologies, PTU, Punjab

---

Abstract - VANET contains vehicle and devices placed on roads is called Road-Side Unit (RSU).The wireless transmission and receiving of data done by device is called on board unit (OBU). The transmission between vehicle and RSU is made possible by OBU. The data or message transmission between two moving vehicle is called vehicular Ad Hoc Network .Since there is frequent change in network therefore the topology does not remain due to which it is called as Vehicular Ad hoc network or temporary network. A Vehicle to Vehicle communication is called V2V and communication between infrastructure and vehicle is called V2I. The road side accident are increase day by day so to reduce accident VANET play important role in reducing accident on road. One of the main challenges within the style of vehicular ad-hoc network is that the developments of a dynamic routing protocol which will facilitate broadcasting within the nodes. While transmission between Vehicles and Vehicles to road side unit the privacy of data message should be taken in concern. It is important to check whether the message sent by sender is authentic or not before sending to receiver. The authenticity of data sender should be checked by authority for efficient transmission. The technique is proposed in which every node will maintain its Data Routing Information (DRI) table by applying New Route Discovery (NRD) Technique. The Data Routing Information (DRI) table will contain the ID of nodes which will contain secure route path from source to destination.

Key Words: VANET, NRD, DRI

1. INTRODUCTION

VANET is a particular kind of MANET that allows information transfer between neighboring vehicles (V2V) and nearby fixed roadside unit (RSU) to make Vehicle to Road (V2I) communication [7]. A vehicle can communicate with another vehicle directly which is called Vehicle to Vehicle (V2V) communication, and vehicle can communicate with an infrastructure such as a Road Side Unit (RSU), known as Vehicle-to-Infrastructure (V2I) communication. VANET consists of moving vehicles communicating with each other as well as with some nearby RSU [18]. These kinds of communications may facilitate to stop the accidents, the analysis of post accident or traffic congestion by permitting vehicles to share and broadcast security info with alternative vehicles to notify the drivers and additionally could facilitate to acquire the weather information, traffic, and real time news [7].

2. ARCHITECTURE OF VANET

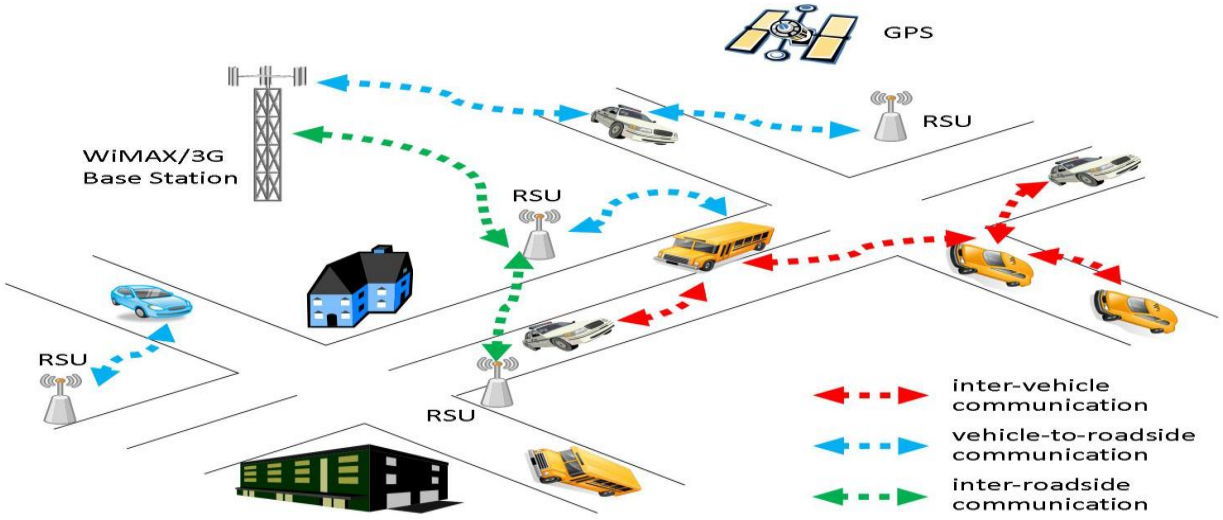


Fig: - Architecture of VANET [13]

The elements needed in VANETs are On-board Unit, Application Unit and Road-side Unit. An On-board Unit is an equipment that exist in vehicle and aids in distribution of info with RSUs or with additional OBUs. Road-side Unit is a road side infrastructure that could be permanent beside roads junctions, parking slots, fuel pumps, intake joints, etc. It consist of a device with networking facilities that employ for short range wireless communications with IEEE 802.11p.An Application Unit is an equipment that reside in vehicle and perform applications using the commuting abilities of the OBU [10].

3. SECURITY IN VANET

Vehicular Ad hoc Networks (VANETs) are appearing as the most popular network layout for Intelligent Transportation Systems (ITS), providing intercommunication between close vehicles in the support of web connection, in addition to a diversity of security applications [17]. When a vehicle detect an occurrence like a disaster or accident, terrible road situation because of climate, traffic congestion, etc., it's necessary to transmit that info to vehicles in suitable areas thus their drivers can take applicable steps [1]. The issue is to create a protocol that can send a message from one supply node to every node in her communication vary with the maximum potential reliability and lowest delay. A successful message distribution in VANETs requires an effective decision mechanism so as to increase reliability and keep the overhead low. The decision measure concerning when and how a security message ought to be transfer or continual is an open matter [17]. Malicious, egocentric and interloper drivers can take benefits of alternative cooperative drivers and make use of their belief. Malicious drivers can transmit compromised messages that proclaim bogus statuses of traffic characteristics over the encompassing region. For example, they may mislead alternative drivers by announcing some road segments in extremely crowded situation. The receiving drivers consider that passing through these road segments might utilize additional traveling time and stop following an alternative route approaching their targeted destination. After that, these malicious drivers get pleasure from their trip through a light and comfy traffic atmosphere after directed traffic somewhere else incorrectly. Furthermore, at the signalized road intersection malicious nodes might report a bogus large priority condition (e.g., ambulance, police vehicle), or incorrectly large traffic density. The intelligent traffic light allocates a larger priority for such a flow of traffic wherever the malicious vehicle will pass the road intersection easily. On the other hand, vehicles on different competing flows of traffic endure from additional queuing delay time; this additionally reduces the throughput of the signalized road intersection. At the similar time, interloper might use the collaboration aspect between drivers in these protocols to stalk and chase alternative drivers. The private info concerning the driver visits, destinations and position throughout any period of time are targeted by interloper

[9]. In such conditions, the integrity and authenticity of the messages transmitted by the vehicles need to be verified whereas at the similar time the obscurity of the senders of those messages ought to be preserved i.e. the identities of the vehicles or drivers mustn't be discovered to any other vehicle or driver [1].

4. RELATED WORK

Kiho Lim et al. [2016] stated that the economical or efficient protocols are useful for quick dissemination of genuine or valid messages in VANETs. It ensures the obscurity or secrecy of the senders and also provides mechanism for enforcement agencies to trace the messages to their senders, once necessary. During this protocol, RSUs not solely manifest or authenticate messages sent by vehicles quick; however also distribute messages through another or opposite RSUs to the vehicles within the acceptable areas quickly [1].

Roshan Jahan et al. [2016] stated that the existence of malicious nodes in network impact the network transmission. Malicious nodes generate different category of attacks in network to damage the communication or transmission. Communication in VANET is influenced by various problems, like traffic on road and fast mobility. They present a technique for reliable or valid communication in VANET through well organized routing protocol. The proposed protocol is efficient to verify malicious node in network, and appropriately change the route for packet dissemination [2].

Pandi Vijayakumar et al. [2016] proposed a double authentication method to offer a huge level of safety in the vehicle area to efficiently avoid the unauthorized vehicles getting into the VANET. They additionally present a double group key management technique to effectively assign a group key to a set of users and to update such group keys throughout the users' connect and depart operations [3].

Imen Achour et al. [2015] present a density-based protocol for safety message distribution, known as "Redundancy Based Protocol (RBP)". The objective of this protocol is to cope with the broadcast storm problem by minimizing excessive broadcasts whereas providing high packet reachability and a low end-to-end delay in a highway atmosphere. It takes into consideration the neighboring vehicles' density throughout the broadcasting procedure with a particular metric, named "Packet Redundancy Ratio", computed locally at every vehicular node. On the premise of this metric, every vehicle is capable to dynamically identify the probability of rebroadcast in order to alleviate the broadcast storm problem [8].

Chaker Abdelaziz Kerrache et al. [2016] present a latest resolution for the detection of intellectual malicious behaviors based on the adaptive detection threshold. They proposed a brand new trust-based method using threshold adaptive control scheme to deal with attackers that intellectually adapt and vary their behavior to keep away from the detection and to escape elimination from all network operations [4].

Chan-Ki Park et al. [2013] analyze communication rate of various data packet size in Vehicular Adhoc Networks. At the results, there exists a distinction in communication effectiveness. Therefore, when VANETs broadcast information to neighbor nodes, data packet size is extremely significant issue for enhancing VANETs performance [14].

Dr.Parminder Singh [2014] calculate the performance of vehicular ad hoc network using different QOS metrics, which influence the performance of network transmission, and additionally examine the QoS performance using metrics routing overhead, packet delivery ratio and average delay with 1024 bytes packets for unicast routing protocols and multicast routing protocols in urban atmosphere. They examine the performance of Dynamic Source Routing (DSR), Ad hoc on demand Distance Vector routing (AODV), Adaptive Demand driven Multicast Routing (ADMR), and On Demand Multicast Routing Protocol (ODMRP). After estimation, results are compared with 512 bytes packets to observe the distinction in performance of vehicles with various packet sizes [11].

Sisily Sibichen et al. [2013] present an effective Adhoc On-demand Distance Vector (AODV) protocol that eliminates the harmful node by separating it, thereby ensuring safe information transmission. Nodes can connect or depart at any time in adhoc network therefore an effective safety measures are required. So, the nodes are organized in spanning tree manner. An RSA key exchange and two encryption methods are used between authorized neighbours in the adhoc network to offer additional security and therefore keep away from group rekeying issues [15].

Shubham Mittal et al. [2016] present a method to enhance the adaptability of the protocol with the dynamic topology. Since vehicle/node in Vehicular adhoc network is a high-speed moving entity, therefore the path between the nodes splits commonly. The algorithm creates an alternate path for the information packet dissemination when link split happens. This method enhances the flow rate of information packets in the network and reduces the end-to-end delay. The simulation is accomplished to estimate the network performance, and the result of AODV-AP demonstrates the high packet delivery ratio and lesser network overhead as compared to AODV and OLSR [5].

N Rajashekar et al. [2016] discusses on how to broadcast the packets safely in adhoc networks. The dissemination of packets relies upon the size of the data for broadcasting. The delay is caused in encrypting large quantity of information. To keep away from this delay, they converse different techniques used on how to encrypt and offer protection for little fragments of information, in order to decrease the communication delay. Decryption and de-fragmentation of information is accomplished at destination end. The packets which are disseminate throughout the routing path, is made protected, so as to prevent the loss of packets within the network. By performing the safe routing, the effectiveness in dissemination of packets will be enhanced and the packets will be disseminated with reduced information loss in the network [6].

Ankit Kumar et al. [2014] discussed the security requirements in VANETs such as Confidentiality, Data Integrity, Non-repudiation, Authentication, Availability and Access Control. They also discuss the attacks to Authentication, Availability, Confidentiality, Data Integrity and Access Control. They present framework to offer security in Vehicular adhoc network [12].

Dr. L. G. Malik et al. [2013] presents the analysis of worldwide research work on different problems associated to VANET; challenges, stability, performance parameters and solutions to them [16].

5. PROPOSED METHODOLOGY

The main work of proposed methodology is to found reliable path between nodes for transmission .The proposed methodology work in two phases

5.1. Malicious Node Detection

5.2. New Route discovery (NRD) Technique

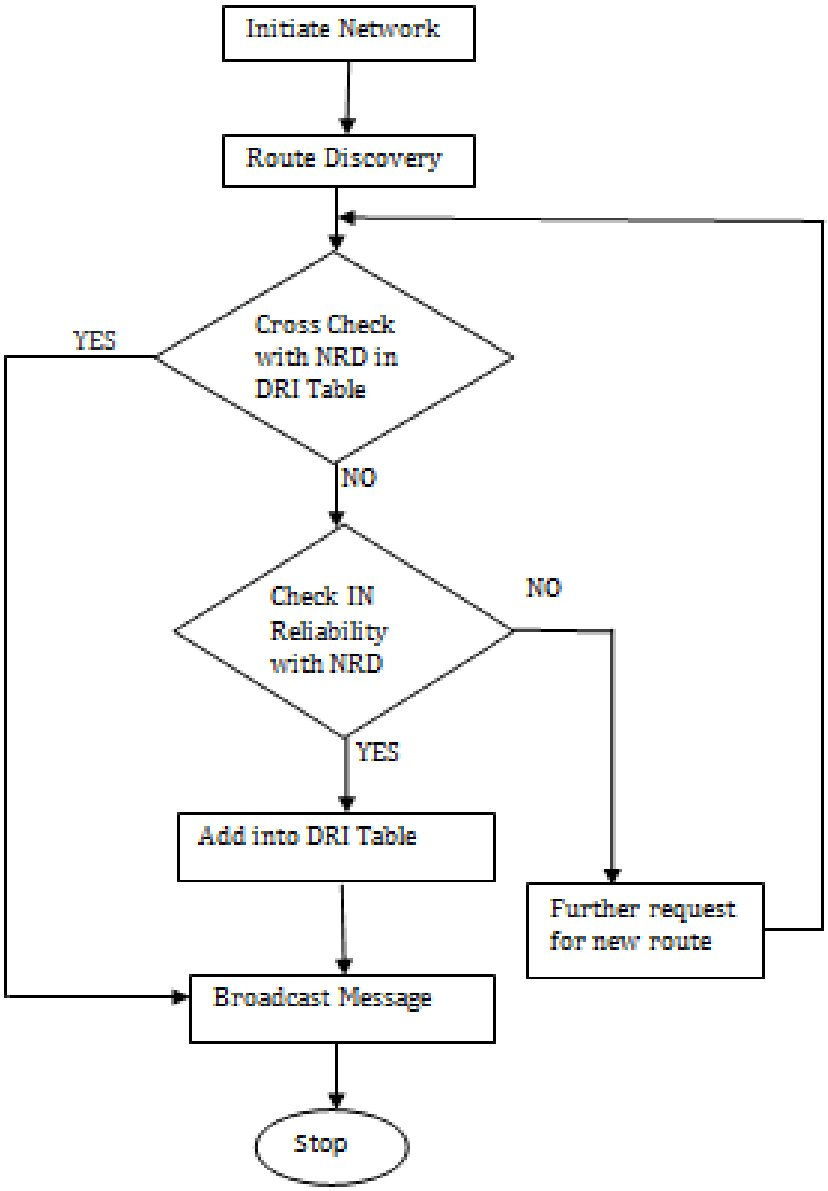
5.1. Malicious Node Detection

1. To initiate the network, the movement of the nodes will be displayed in simulation area.
2. Data from source node to destination node is send by generating path. Intermediate nodes are lying between source and destination node. Source node sends Route Request (RREQ) Packet to find the path.
3. When there is no reply from any node within given time or the node take time to send data then source node will considered it as malicious node.
4. If any intermediate node reply for path from source to destination node but it drops packets then that node will be considered as malicious node.
5. If intermediate node un-route packet from source to destination after sending Route Reply (RREP) Packet to source node then that node will be considered as malicious node.

5.2. New Route discovery (NRD) Technique

1. After initiating network, every node will maintain its Data Routing Information (DRI) table by applying New Route Discovery (NRD) Technique.
2. The Data Routing Information (DRI) table will contain the ID of nodes which will contain secure route path from source to destination.
3. If intermediate node within the network already exist in Data Routing Information (DRI) table of sender node then sender node will send data to the intermediate node.

FLOWCHART:-New Route Discovery (NRD) Technique



ALGORITHM: New Route Discovery (NRD) Technique

N= No of Route Discovered, NRD= New Route Discovery, DRI= Data Routing Information

1. for time = 1 to simulation time
2. for i= 1:N, where N Route Discovery
3. Route Discovery with NRD Technique
4. if (Route Find)
5. Add Node ID in DRI Table
Else
6. Request for New Route
Else
7. Broadcast Message
8. endif
9. end

Configuration Table used for Evaluation of Results

S.No.	Parameter	Value(s)
1	Simulator used	NS 2.35
2	Simulation Time	10 Secs
3	Simulation Area	1000 X 1000
4	MAC	802.11
5	Number of nodes	30
6	Number of RSU	3

6. RESULT ANALYSIS

The aim of our proposed technique is to decrease message transmission overhead. The communication between vehicle to vehicle and vehicle to RSU is done in our proposed Technique. The reliable nodes are identified in vehicle to vehicle and vehicle to RSU communication .The reliable nodes are identified by NRD technique and DRI Table is maintained with reliable nodes. The optimal path is generated in DRI table which is used for communication between various nodes and RSU, the DRI table help in reducing message retransmission and better transmission in VANET. The comparison result between previous technique and proposed technique shown in fig 1,2,3 and Table 1,2,3 for 10, 20, and 30 Vehicles. The results show that proposed technique has better performance than previous technique.

Message overhead for 10 Vehicles: The comparison result between previous technique and proposed technique has shown in fig 1 and Table 1 for 10 Vehicles. The result show that proposed technique has better performance than previous technique as message transmission increases the overhead result value for previous technique is higher as compared to Proposed Technique.

Fig 1: comparison of message overhead for 10 vehicles

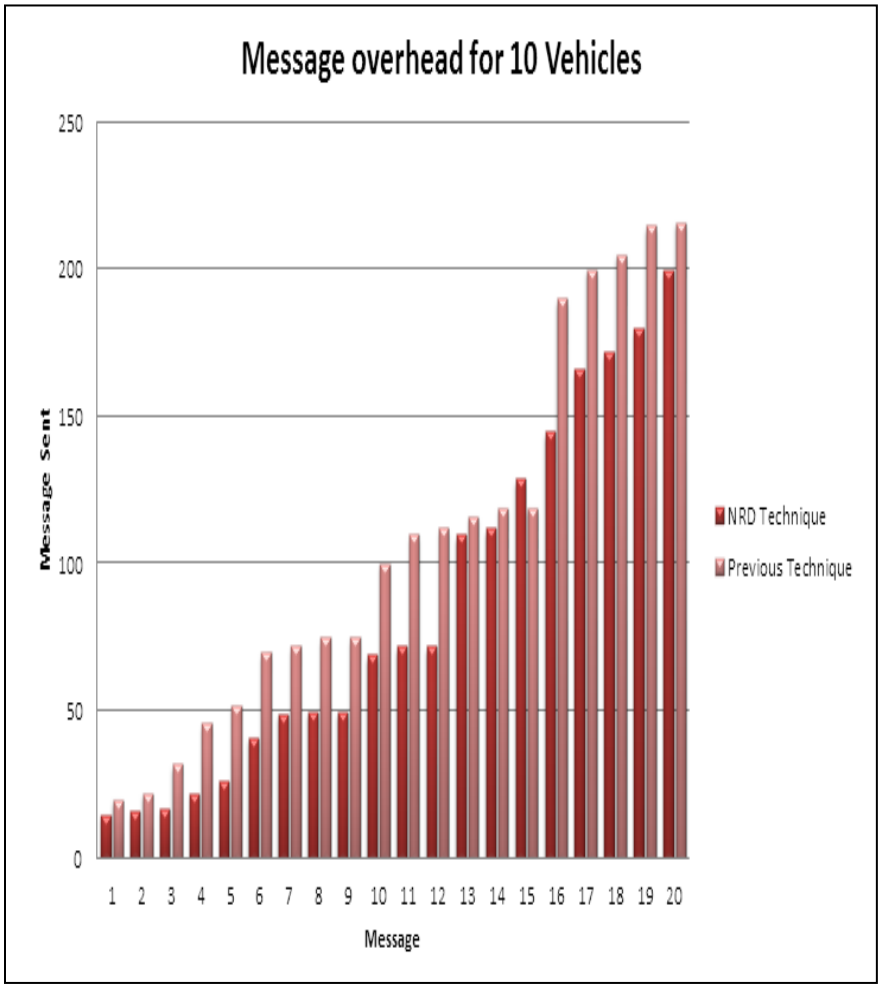


Table 1: comparison of message overhead for 10 vehicles

Message Sent	NRD	Previous Technique
1	15	20
2	16	22
3	17	32
4	22	46
5	26	52
6	41	70
7	49	72
8	50	75
9	50	75
10	69	100
11	72	110
12	72	112
13	110	116
14	112	119
15	129	119
16	145	190
17	166	200
18	172	205
19	180	215
20	200	216

Message overhead for 20 Vehicles: The comparison result between previous technique and proposed technique shown in fig 2 and Table 2 for 20 Vehicles. The result shows that proposed technique has better performance than previous technique. Overhead value of previous technique increases with the increase in no of vehicles. The performance while with the 20 no of nodes the evaluation values of message overhead of proposed technique is less as compared to previous technique.

Fig2: comparison of message overhead for 20 vehicles

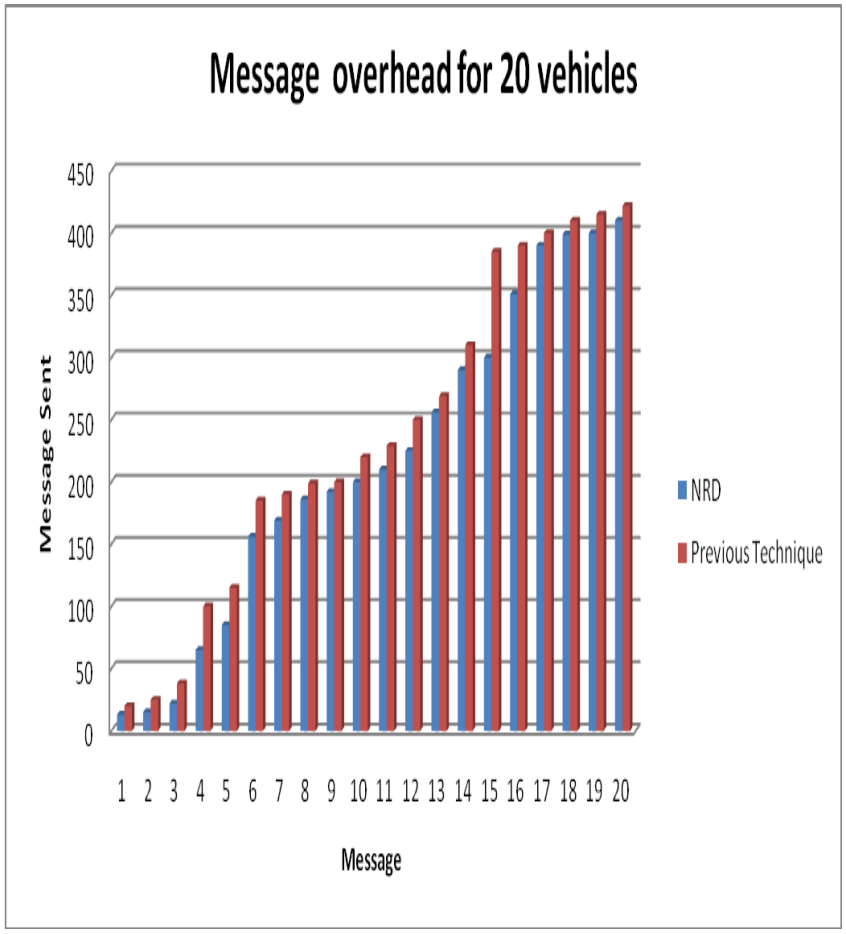


Table 2:comparison of message overhead for 20 vehicles

Message Sent	NRD	Previous Technique
1	13	20
2	15	25
3	22	38
4	65	100
5	85	115
6	156	185
7	169	190
8	186	199
9	192	200
10	200	220
11	210	229
12	225	250
13	256	269
14	290	310
15	300	385
16	351	390
17	390	400
18	399	410
19	400	415
20	410	422

Message overhead for 30 Vehicles: The comparison result between previous technique and proposed technique shown in fig 3 and Table 3 for 30 Vehicles. The results show that proposed technique has better performance than previous technique.

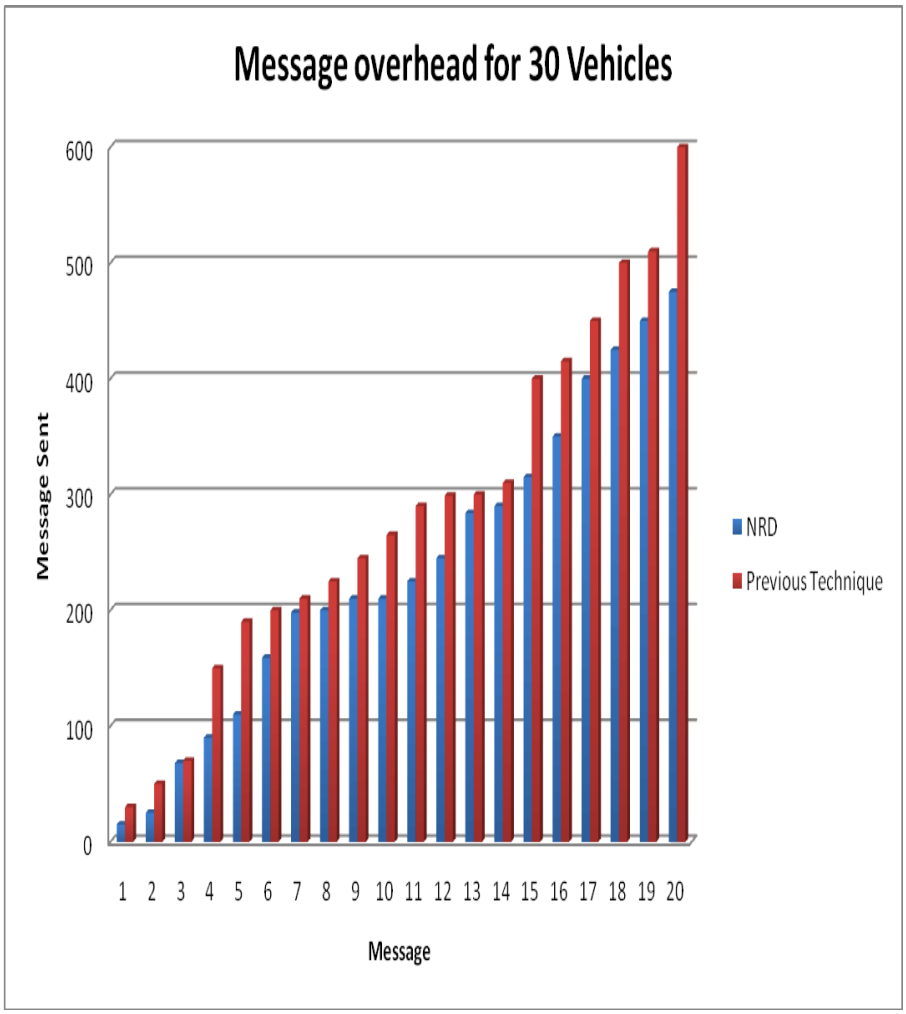


Fig 3: comparison of message overhead for 30 vehicles

Message Sent	NRD	Previous Technique
1	15	30
2	25	50
3	68	70
4	90	150
5	110	190
6	159	200
7	198	210
8	200	225
9	210	245
10	210	265
11	225	290
12	245	299
13	284	300
14	290	310
15	315	400
16	350	415
17	400	450
18	425	500
19	450	510
20	475	600

Table 3: comparison of message overhead for 30 vehicles

7. CONCLUSION:

The DRI Table technique is proposed in which every node will maintain its Data Routing Information (DRI) table by applying New Route Discovery (NRD) Technique for VANET. The Data Routing Information (DRI) table will contain the ID of nodes which will contain secure route path from source to destination. If intermediate node within the network already exist in Data Routing Information (DRI) table of sender node then sender node will send data to the intermediate node. The proposed technique will remove non secure path which help in increasing throughput and packet delivery ratio of network. The proposed algorithm continuously updates the routing table. The proposed technique will reduce the overall congestion. The proposed algorithm provides detail evaluation of message overhead. Our proposed technique provide better solution than previous technique.

REFERENCES

1. K. Lim, D. Manivannan, "An efficient protocol for authenticated and secure message delivery in vehicular adhoc network",http://dx.doi.org/10.1016/j.vehcom.2016.03.001, Veh. Commun (2016)

2. Roshan Jahan, Preetam Suman, "Detection of malicious node and development of routing strategy in VANET", 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), pp 472-476(2016)

3. Pandi Vijayakumar, Maria Azees, Arputharaj Kannan, and Lazarus Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular AdHoc Networks", IEEE Transactions on Intelligent Transportation Systems, Vol.17, No.4, April 2016.

4. Chaker Abdelaziz Kerrache, Abderrahmane Lakas, Nasreddine Lagraa, "Detection of Intelligent Malicious and Selfish Nodes in VANET using Threshold Adaptive Control", 978-1-5090-5306-3/16/$31.00 c 2016 IEEE.

5. Shubham Mittal, Ramandeep Kaur, Kamlesh C.Purohit, "Enhancing the Data Transfer Rate by Creating Alternative Path for AODV Routing Protocol in VANET", 978-1-5090-3480-2/16/$31.00 ©2016 IEEE

6. Arun Nagaraja, Nimmala Mangathayaru, N Rajashekar, T Satish Kumar, "A Survey on Routing Techniques for Transmission of Packets in Networks", 978-1-5090-5579-1/16/$31.00 c 2016 IEEE.

7. Tareq Emad Ali, Layth A. Khalil al dulaimi, Yamaan E. Majeed, "Review and Performance Comparison of VANET Protocols: AODV, DSR, OLSR, DYMO, DSDV & ZRP", 2016 AI-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AICMITCSA)-IRAQ (9-10) May.

8. Imen Achour, Tarek Bejaoui, Anthony Busson, Sami Tabbane, "A Redundancy-based Protocol for Safety Message Dissemination in Vehicular Ad Hoc Networks", 978-1-4799-8091-8/15/$31.00 ©2015 IEEE.

9. Maram Bani Younes, Azzedine Boukerche, "SCOOL: A Secure Traffic Congestion Control Protocol for VANETs", 2015 IEEE Wireless Communications and Networking Conference (WCNC):- Track 3: Mobile and Wireless Networks, 978-1-4799-8406-0/15/$31.00 ©2015 IEEE.

10. Parul Choudhary, Umang, "A Literature Review on Vehicular Adhoc Network for Intelligent Transport", 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), 978-9-3805-4416-8/15/$31.00_c 2015 IEEE.

11. Dr.Parminder Singh, "Comparative Study between Unicast and Multicast Routing Protocols in different data rates using Vanet", 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 978-1-4799-2900-9/14/$31.00 ©2014 IEEE

12. Ankit Kumar, Madhavi Sinha, "Overview on Vehicular AdHoc Network and its Security Issues", 2014 International Conference on Computing for Sustainable Global Development (INDIACom), 978-93-80544-12-0/14/$31.00_c 2014 IEEE

13. Raj Jain, "Introduction to Vehicular Wireless Networks", Washington University in St. Louis, pp.8-9 (2014)

14. Chan-Ki Park, Kuk-Hyun Cho, Min-Woo Ryu, Si-Ho Cha, "Measuring the Performance of Packet size and Data rate for Vehicular Ad Hoc Networks", 978-1-4799-0604-8/13/$31.00 ©2013 IEEE

15. Sisily Sibichen, Sreela Sreedhar, "An Efficient AODV Protocol and Encryption Mechanism for Security Issues in Adhoc Networks", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013) 978-1-4673-5149-2/13/$31.00 ©2013 IEEE

16. Komal Mehta, Dr. L. G. Malik, Dr. Preeti Bajaj, "VANET: Challenges, Issues and Solutions", 2013 6th International Conference on Emerging Trends in Engineering and Technology", 978-1-4799-2560-5/13 $31.00 ©2013 IEEE, DOI 10.1109/ICETET.2013.18

17. Anna Maria Vegni, Alessio Stramacci, and Enrico Natalizio, "SRB: A Selective Reliable Broadcast Protocol for Safety Applications in VANETs", 2012 International Conference on Selected Topics in Mobile and Wireless Networking", 978-1-4673-0937-0/12/$31.00 ©2013 IEEE

18. Sabih ur Rehman, M. Arif Khan, Tanveer A. Zia, Lihong Zheng, "Vehicular Ad-Hoc Networks (VANETs) - An Overview and Challenges", Journal of Wireless Networking and Communications 2013, 3(3): 29-38