ISSN No. 0976-5697

Volume 5, No. 6, July-August 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Trusted Border-node based Most Forward within Radius Routing Protocol

Khushdeep Singh*, Sanjay Batish*, Alka Jindal*
*Dept. of Comp. Science, PEC University of Technology,
Chandigarh, India

Amardeep Singh
Dept. of Comp. Science,
UCOE, Punjabi University,
Patiala, India

Abstract— Increased vehicular traffic demands smart vehicles which can interact with each other and roadside infrastructure to prevent accidents. Vehicular Ad-hoc Network (VANET) provides this flexibility to the vehicles. B-MFR is a position based routing protocol in VANET which forward packets by optimizing the path length by selecting the border nodes. But if two nodes are equidistant from the source node, an ambiguous situation arises. To solve this ambiguity, a new position based routing protocol Trusted Border-node based Most Forward within Radius (TB-MFR) is proposed in this paper.

Keywords— TB-MFR; B-MFR; Packet Delivery Ratio;

I. INTRODUCTION

Today millions of people around the world die every year due to road accidents. Some people are suffering from fatal injuries caused during the road accident [1].Different types of vehicles like trucks, buses, cars etc are running on the road at a given time [2]. To improve safety between different types of vehicle, we need to reduce vehicular traffic accidents and manage the traffic system efficiently. Computer networking researchers proposed a new wireless networking concept for vehicles called Vehicular Ad hoc Network (VANET). VANETs are a special class of mobile ad hoc wireless networks (MANETs). VANET provides safer and well organized road by communicating information in timely manner to drivers and the concerned authorities [3]. VANET plays an important role in traffic management and providing emergency information among vehicles moving on roads. The traffic information is used by various other vehicular applications like safety applications, route guiding applications etc [4].

VANETs will reduce road injury to a larger extent by providing important knowledge to drivers. The knowledge is provided by one vehicle to other vehicle using inter-vehicle communication (IVC) or vehicle to roadside unit via Roadside-vehicle communication (RVC) [5]. To make VANETs successful, routing of such messages demands high attention. VANETs use the standard short range wireless communication IEEE 802.11p (modified version of IEEE 802.11a standard protocol) for communication [6]. This wireless communication protocols are specially designed for vehicular ad-hoc networks (VANETs) that supports safety and non-safety applications.

Routing is the process of finding optimal path between source and destination node and then sending message in time because time is a crucial factor. Routing of messages in VANET is an important part. Routes between source and destination node may contain a single hop or multiple hops. Many routing protocols are used in VANETs like Topology Based Routing Protocol, Position Based Routing Protocol, etc. Topology Based Routing Protocol uses the information about the links among the vehicular nodes which exist in the network to perform packet forwarding. Position Based Routing Protocol uses the neighbor's and destination's location information to perform the packet forwarding. The topology of VANET changes over time due to highly mobile vehicular nodes. It causes frequent network partition and makes communication more difficult in VANET. In a highly dynamic network like VANET, it is considered that Position based routing protocols are more suitable than Topology based routing protocols [7]. Position-based routing protocols like GPSR, GPSR+AGF, GRANT, GPCR, CBDRP, B-MFR, etc are the most reliable protocols [8]. But still a lot of research needs to be done in this field and is attracting many researchers.

In this paper we have proposed an optimization of Border-node based Most Forward with in Radius (B-MFR) routing protocol of VANET. B-MFR uses the concepts of border node of the sender's communication range to minimize the hops between source and destination. But if there are two border nodes which are at equal distance from the destination, no approach is suggested by B-MFR to handle this situation. This problem is solved by the new proposed method, which will choose the node on the basis of trust levels.

The paper is structured as follows: Section 2 presents an overview of B-MFR. Section 3 discusses the proposed algorithm Trusted B-MFR. Section 4 represents the simulation results and performance analysis of the proposed protocol. Section 5 is about conclusion.

II. BORDER-NODE BASED MOST FORWARD WITHIN RADIUS PROTOCOL (B-MFR)

Most Forward with in Radius (MFR) routing protocol uses the position information of the nodes for finding the route. The neighbor with the greatest progress towards the destination is chosen as the next hop for sending the packet [9]. B-MFR is a modified version of MFR routing protocol that uses border nodes with maximum progress. Border node are that nodes which are at Ro distance from the source or forwarding node where Ro is the communication range of source or packet forwarding node. B-MFR reduces the overhead of the source or the forwarding node as they have to look upon the border nodes only to forward packets and not on the interior nodes within the transmission range [10].

A packet is sent to the border node which has the greatest progress on the line drawn from source to destination. In big cities, there is a high probability that two nodes on the border give same progress from a particular node to the destination node. This ambiguity is a problem in B-MFR which can be solved by choosing the node randomly. But this is not an efficient approach to choose the node randomly. To solve this ambiguity we need to modify B-MFR.

The problem is shown diagrammatically below

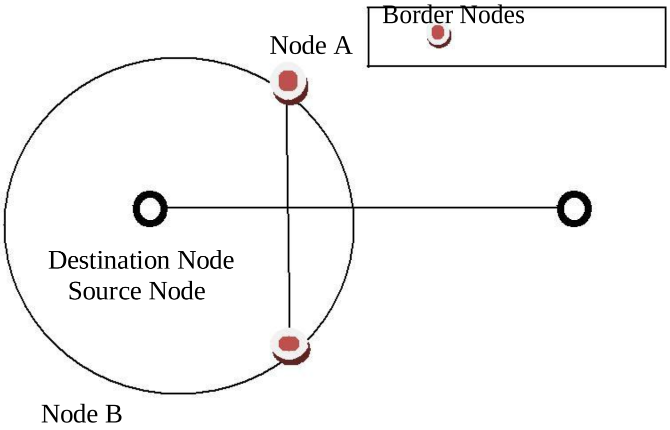

Figure 1 B-MFR routing protocol

As shown in figure 1 above, the two border nodes A and B are equidistant from source and destination. Now the conflict is which one should be chosen? Although, the easiest strategy would be to do it randomly yet it will not be efficient enough.

III. TRUSTED BORDER-NODE BASED MOST FORWARD

A. *Within Radius Routing Protocol (Tb-Mfr):*

The TB-MFR is introduced in this paper which is similar to B-MFR as it takes the border node as the next node. The difference lies in the solution of the problem of ambiguity when two equidistant border nodes come into picture. In that case, it checks trust value of ambiguous border nodes and selects the one which is more trusted. The total packets that are transmitted, received and dropped by the node are taken into account for calculating the trust level. For a particular transmission, it decides which node is going to participate in routing based on their trust values which is calculated based on the total packets handled by each node. Based on this trust value a node is selected from two equidistance node [11].

$$T_i = (trs - trf / trs + trf) \qquad (1)$$

Where, Ti is the trust level value of node i.

Where trs is defined as the packets received successfully by the node i from its neighboring nodes and trf is the packet failure rate which is calculated as the number of packets drop by node i which are send by its neighboring nodes.

The TB-MFR protocol design is based on the following assumptions:

a. Packets forwarding using Border nodes.
b. Every node assigns a trust value and border is selected based on their trust value.
c. Control messages Hello (beacon) are exchanged between next-hop neighbors
d. Nodes (vehicles) are equipped with GPS receiver, digital map and sensors.

In table 1, complete algorithm of Trusted Border-node based Most Forward with in Radius Routing Protocol (TB-MFR) is shown.

Table 1. Algorithm of proposed tb-mfr routing protocol

Notations:
PN: present forwarding node

NPN: Set of neighbors of present forwarding node
T_i: trust value of i-th node.
LSN: List of selected nodes

SNN: selected next forwarding node
R_0: Max communication range
S is original source node
Algorithm:
1) PN = S
2) Check if the destination is in the Communication range of PN then send packet to destination node and exit.
3) SNN = Null
4) Compute Euclidian distance of all nodes in NPN from node PN
5) For all Ni € NPN, i ← 1 to n
{ if (distance of Ni from PN == R0)
Add Ni to LSN}
6) Find the projection of all nodes in LSN on the line which join source node and final destination node (A-axis).
7) Ni is a node which having maximum projection on A-axis.
8) if two node Ni and Nj have same maximum projection
{Compute the Trust value Ti of Ni and Tj of Nj node.}
9) if (Tj > Ti)
SNN← Nj
10) else
SNN← Ni
11) if (SNN == Null)
Repeat 4 - 11
Else
{
Forward the packet to SNN
PN = SNN
Repeat 2 - 11 }
12) End

IV. SIMULATION RESULTS AND PERFORMANCE

A. *Analysis:*

To evaluate the performance of TB-MFR protocol, it is implemented using NS-2.33 simulator and simulations are conducted. We compare TB-MFR with B-MFR, AODV and DSR (Dynamic source routing) routing protocol in vehicular environment. Based on the simulation parameters given below, we simulate the protocol with a transmission range of 250m. We consider a open traffic scenario where vehicles are moving in every direction. The IEEE 802.11 DCF (Distributed Coordinated Function) is used as the MAC protocol. We use a 2500m * 800m square area for simulation. Network size is represented by the number of vehicles. The traffic density is not uniform and it depends on the number of vehicles chosen in the given area. The packet transmission density can be adjusted by setting different CBR rates with a packet size of 1000 bytes. A simulation runs for 200 seconds and we have taken average of 5 simulation runs.

Table 2. Parameter Values

Simulation time	200s
Simulation area	2500m*800m
No. of vehicles	10, 20, 30
Transmission range	250m
Packet size	1000 bytes
Traffic type	CBR (Constant bit Rate)
MAC protocol	IEEE 802.11 DCF

A. Packet Delivery Ratio (PDR):

It is the number of successfully delivered data packets out of total number of data packets sent. It can be observed from Figure.2 that TB-MFR outperform then B-MFR, AODV and DSR in terms of PDR. This improved performance of TB-MFR can easily be explained by understanding the significance of using Trust value of equidistant border nodes. In case of TB-MFR higher trusted border node is selected for forwarding data which selects the node which drops fewer packets as compared to other. Therefore, PDR to deliver the packet successfully from source to destination is increased.

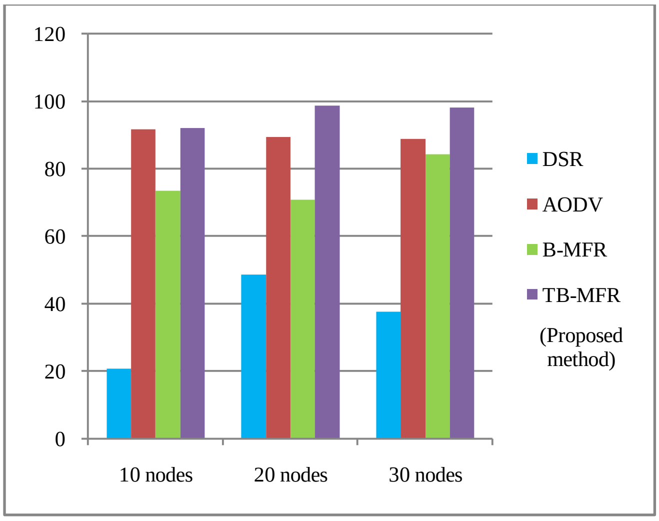

Figure 2 Packet Delivery Ratio

B. End to End Delay:

This metric is defined as the average delay incurred in the transmission of all data packets delivered successfully. The end to end delay characterizes the latency generated by the routing approach this include every type of delay that occur during transmission. These are some following types of delay:

a. Transmission delay
b. Propagation delay
c. Processing delay
d. Queuing delay

All these delays occur at each node which participate in route path to transmit data. So, end to end delay is derived as:

End to End delay = NL(TD + PD + PrD + QD), where
NL = Number of Links
TD = Transmission delay
PD = Propagation delay
PrD = Processing delay
QD = Queuing delay

Lower the End to End delay means a protocol is better. In case of TB-MFR End to End delay is low as comparison to DSR and AODV routing protocols but it is slightly higher than B-MFR.

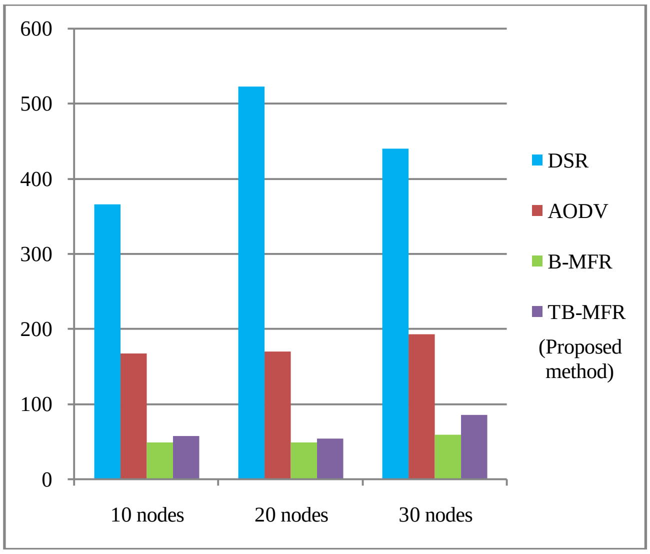

Figure 3 End to End Delay

V. CONCLUSION

In this paper we proposed a routing protocol TB-MFR which takes the benefit of B-MFR. TB-MFR improves the throughput as compared to B-MFR because TB-MFR selects the node on basis of trust value and trust value for any node becomes low if that node drops packets. If we have two equidistant nodes form source and destination, then we select the node with higher trust value to forward the packet. This approach results in reducing the total number of packets dropped and hence will result in increased packet delivery ratio of the network.

IV. REFERENCES

[1] Ruikar Manisha, "National statistics of road traffic accidents in India",Journal of Orthopaedics and Traumatology and Rehabilitation Vol.6 No.1, Sep 2013.

[2] H.Moustafa Zhang Yan, "Vehicular networks: Techniques, Standards, and Applications," CRC Press, 2009.

[3] S S MANVI and M S KAKKASAGERI, "Issue in Mobile Ad hoc Networks for Vehicular Communication," IETE Technical Review, March-April 2008.

[4] Muhammad Shoaib, Wang-Cheol Song "Traffic Aware Optimized Zone based Hierarchal Link State Routing Protocol for VANET", IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Mobile and Wireless Networks, 2013.

[5] Fan Li and Yu Wang, "Routing in Vehicular Ad Hoc Networks: A Survey", University of North Carolina, IEEE Vehicular Technology Magazine, June 2007.

[6] Qi Chen, D. Jiang, V. Taliwal, and L. Delgrossi, "IEEE 802.11 based Vehicular Communication Simulation Design for NS-2," VANET' 06, Los Angeles, California, USA, September 29, 2006.

[7] J. Chennikara-Varghese, W. Chen, O. Altintas, S. Cai, "Survey of routing protocols for inter-vehicle communications," 3rd Annual International Conference on

Mobile and Ubiquitous Systems -Workshops, 2006.

[8] Book of Kevin C. Lee, UCLA, USA Uichin Lee, UCLA, USA Mario Gerla, UCLA, USA,“Survey of Routing Protocols in Vehicular Ad Hoc Networks”.

[9] I. Stojmenovic, A. P. Ruhil, and D. K. Lobiyal, “Voronoi diagram and convex hull based Geocasting and routing in wireless networks,” Wireless Communications and Mobile Computing, John Wiley & Sons Ltd, 2006.

[10] Ram Shringar Raw, D K Lobiyal, “B-MFR Routing Protocol for Vehicular Ad hoc Networks”, International Conference on Networking and Information Technology 2010.

[11] Sridhar Subramanian and Baskaran Ramachandran “QOS ASSERTION IN MANET ROUTING BASED ON TRUSTED AODV (ST-AODV)”, International Journal of Ad hoc, Sensor & Ubiquitous Computing.

