International Conference on Latest Innovation in Engineering Science and Management
Buddha Institute of Technology, GIDA, Gorakhpur (UP)
30th - 31st March 2019 www.conferenceworld.in
ISBN : 978-93-87793-80-4

Multipath Routing Protocol with Selfish Node Detection by using Cluster Based Reputation Technique

Prashant Kumar Tripathi[1] and Alok Bhatt[2]

[1]Department of Information Technology,
National Institute of Electronics and Information Technology, Gorakhpur, India
[2]Department of Computer Science & Engineering,
Buddha Institute of Technology, Gorakhpur, India

Abstract: Mobile Ad-hoc Networks (MANETs) is self configured and decentralized wireless network without any predefined infrastructure [1]. Every node acts as a router so routing may be more difficult in MANET due to freely movement of nodes. Most of the routing algorithms designed for MANET are based on the assumption that every node forwards every packet but in practice it may not possible because some of the nodes may act as the selfish nodes which use the network and its services but they do not cooperate with other nodes. This paper basically based on the concept of multipath routing in which we have evaluated the performance of a widely used on-demand multipath routing protocol called AOMDV with Selfish Node Detection (SND) using cluster based reputation technique. The selfish nodes have detected by dividing the networks into small clusters restricted within one hop distance and assuming the lowest mobility node as cluster head. The cluster head decides the selfishness of a node by monitoring the reputation value. In multipath scenario, AOMDV has been selected due to efficiency over other protocols in aspects of reducing routing load, delay, etc. The evaluation of AOMDV protocol by detecting selfish nodes is carried out in terms of data packet loss, average end to end delay and throughput.

Keywords: AOMDV, Cluster Head (CH), MANET, Reputation Based System, Selfish nodes.

I. INTRODUCTION

In a mobile ad hoc network (MANET), each node has to support other node to deliver its packets. To have smooth communication within the network, a routing protocol is used to establish routes between intermediate nodes without any error prone situation. The primary goal of such ad-hoc network routing protocol is to maintain trust and reliability within network by establishing correct and efficient route between pair of nodes so that messages can be delivered in a timely manner. As in MANET, mobile nodes are commonly depends on computing and power resources, some nodes refuse to cooperate in communication as a result this kind of misbehaviour affects the fairness, reliability and efficiency in MANET. The motivation behind this paper is to detect this kind of nodes which are not cooperative and cause unnecessary delay.

In order to improve the performance of the network in multipath routing (AOMDV), the selfish nodes detection mechanism followed cluster based reputation technique which have discussed in this paper.

The routing protocols in MANET are majorly classified into two categories: Unipath and Multipath routing protocols [4].

A. Concept of Multipath Routing

In recent years, on-demand routing protocols have attained more attention in mobile Ad hoc networks as compared to other routing schemes due to their abilities and efficiency. However, mostly protocols use a single route discovery process and do not utilize multiple alternate paths. There are three key objectives to designing a multipath routing protocol that operates successfully by handling the challenges of an Ad hoc network [8]:

1. In highly dynamic environment the table-driven protocol is not suitable since it increase network overhead. In present scenario the protocol must be on-demand, meaning that it has to react to changes in the environment only when necessary. The AOMDV served the same.

2. The protocol must involve multiple paths between source and destination because when a path breaks an alternate path can be used instead of initiating a new route discovery. Multipath routing must also achieve load balancing, lower end-to-end delay and must be

more resilient to route failures and also avoid congestion problems.

3. The detection of uncooperative nodes make it more efficient in terms of reliability and performance aspects as discussed in this paper.

B. *AOMDV (Ad Hoc On-demand Multipath Distance Vector Routing Protocol)*

To eliminate the occurrence of frequent link failures and route breaks in highly dynamic ad hoc networks, AOMDV has been developed from a unipath path on-demand routing protocol AODV. The AOMDV [1,4] protocol finds multiple paths and this involves two stages which are as follows: i) A route update rule establishes and maintains multiple loop-free paths at each node, and ii) A distributed protocol finds link-disjoint paths. The AOMDV protocol finds node-disjoint or link-disjoint routes between source and destination. Link failures may occur because of node mobility, node failures, congestion in traffic, packet collisions, and so on. For finding node-disjoint routes, each node does not immediately reject duplicate RREQs. A node-disjoint path is obtained by each RREQ, arriving from different neighbour of the source because nodes cannot broadcast duplicate RREQs. Any two RREQs arriving at an intermediate node through a different neighbor of the source could not have traversed the same node. To get multiple link-disjoint routes, the destination sends RREP to duplicate RREQs regardless of their first hop. For ensuring link-disjointness in the first hop of the RREP, the destination only replies to RREQs arriving through unique neighbors. The RREPs follow the reverse paths, which are node-disjoint and thus link-disjoint after the first hop. Each RREP intersects at an intermediate node and also takes a different reverse path to the source to ensure link-disjointness.

II. RELATED WORK

In simple multipath routing (SMR) [2], same packet is transmitted to fewer selected paths among all possible paths between source and destination. It increases the number of transmissions and also increases reliability of transmissions of packet at the cost of the number of transmission with increases the traffic overhead. In MRRecoil [2], there is one main path which is called as primary path and the rest paths as recoil path. Initially the packet is transmitted via primary path. If the transmission fails, then same packet is transmitted via recoil path i.e. secondary path. So, here the delay is more but number of transmission is less as compare to the SMR. There are many schemes in the literature which deals with misbehaving nodes and provide solutions.

In reputation based technique [6], network nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network. Credit based technique provides incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency (credit) or similar payment system may be set up.

A. *Research Methodology*

The steps involved in implementing routing protocols are as follows-

1) Developing multipath routing protocol using an object oriented language.
2) Understanding the performance evaluation metrics like throughput, packet delivery ratio, packets dropped and end-to-end delay.
3) Creating mobile nodes by setting and configuring mobile nodes with required parameters.
4) Divide the networking nodes into small clusters and decide a cluster head (CH) within each cluster. The CH is decided on the basis of lowest Mobility Based Metric for Clustering which is based on the assumption that mobile nodes with low speed relative to their neighbours have the chance to become cluster heads.
5) Detecting selfish nodes in routing by using reputation based technique within each cluster.
6) Evaluate the packet loss, throughput and end to end delay of new proposed algorithm.

III. PROPOSED WORK

We proposed an approach for increasing the efficiency of Ad hoc On-demand Multipath routing protocol using trust based route selection process which is decided by obtaining reputation value. The Reputation value is calculated [5] using equation below. Each node calculates the reputation Rpt (i, j) t for each of its neighbour j at time t.

$$\text{Rpt (i,j)}t = \sum_{pkts=0}^{pkts=\infty} F(pkts)/R(pkts) \qquad (1)$$

Where Reputation of i and j at time t is the reputation value calculated by monitoring the neighbour j directly at time t; Fpkts is the number of packets forwarded by node j and Spkts is the number of packets sent by node j. As a result, a node with the

highest reputation will get the chance to participate in communication as decided by cluster head.

A. *Proposed Algorithm*

In cluster based reputation monitoring module continuously monitors node behaviour and assign a reputation values to nodes based on their packet forwarding activity in the routing table. The proposed algorithm is described as follows:

Step 1: Local stability is computed in order to select some nodes as cluster heads (CH). A node may become a cluster head if it is found to be the most stable node among its neighbourhood. Thus, the assumption is based on the concept that, mobile nodes with low speed relative to their neighbours have the chance to become cluster heads.

Step 2: Each CH maintains reputation values of all nodes lie within that cluster at one hop distance and other nodes that have had a transaction with it.

Step 3 A CH observes a packet forwarded by neighbours P and Q as it lies at one hop distance from its neighbouring nodes.. To calculate the reputation value Rpt (P, Q) equal to the ratio of packet delivered by Q to the total number of packets sent by node P as shown in Eqn 1. The information regarding to the reputation value is reflected to CH.

Step 4: A node P can obtain opinion about Q by requesting reputation value Rpt from the CH lie within that cluster or in other words CH can hold the information about all neighbouring nodes (one hop) of its cluster and send the information (Rpt) to P against Q.

Step 5: As a result (calculated by Eqn 1), node with reputation value is greater than threshold value (or higher value of Rpt) can participate in route discovery process as decided by CH.

IV. SIMULATION RESULTS AND ANALYSIS

A. *Simulation Setup*

We evaluate the performance of the proposed mechanism using the Network Simulator (NS-2) and compare it to the existing protocol. A wireless ad hoc network area with the size of 500 m * 500 m have simulated in our proposal. The mobility of nodes considered as "random waypoint" model. In this evaluation, we are mainly focused by estimating data packet loss, throughput and average end to end delay of the network to measure the network performance in the presence of selfish nodes detection mechanism.. Simulation result shows that our proposed approach outcome is better than the existing multipath protocol AOMDV. We set up the following network parameters while simulate our desired work as listed in table 1.

Table 1. Simulation Parameters

Parameter	Value
Number of nodes in the field	100
Simulation Area	500*500
Nodes that send data every time	20
Routing protocol	AOMDV and AOMDV with SND
Mobility patterns	Random Waypoint
Simulation time	50 seconds
MAC Type	802.11
Traffic Type	CBR
Node Speed	20 m/s
Packet size	512 bytes

B. *Performance Evaluation*

The parameters used in our simulation are comparision results of data packet loss, throughput and average end to end delay.

Data Packet Loss

When a source node sends data packet towards its destination node and when it is not delivered to the destination node it is called packet loss. The performance is better when data packet loss is minimum.

Throughput

Throughput is defined as the rate at which the data is transferred from one node to another node in a network. The unit of throughput is bits/sec. The performance is better when throughput is high.

Average End to End Delay

The average time involved in delivery of data packets from the source node to the destination node is called average end to end delay.

Average End to End delay

$$= \sum \frac{(\text{Time received} - \text{Time sent})}{\text{Total Data Packet Received}} \qquad (2)$$

The performance is better when average end-to-end delay is low.

C. Simulation Results:

The results were collected as comparison and we observed that the throughput of our new purposed protocol i.e., AOMDV with selfish node detection (AOMDV with SND) is better than simple multipath routing protocol AOMDV for 20-nodes, 40-nodes, 60-nodes, 80-nodes and 100 nodes scenario. Packet Losses are high for AOMDV routing protocol as comparison to our new protocol in case of 60-Nodes, 80-Nodes and 100- Nodes scenario, Comparative result of Average End to End Delay and throughput show that our proposed protocol is better in network cluster environment and provides a better approach to elect cluster head in reputation based trust environment for detecting selfish nodes.

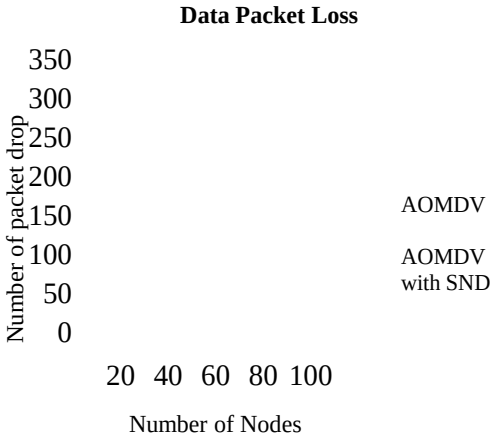

Fig. 1: Packet Loss between AOMDV and AOMDV with SND

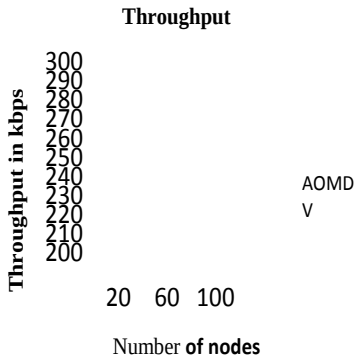

Fig. 2: Throughput between AOMDV and AOMDV with SND

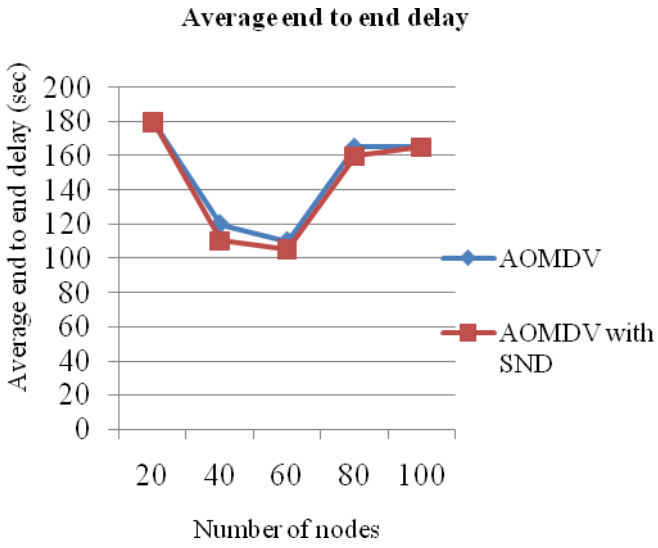

Fig. 3: End to End Delay between AOMDV and AOMDV with SND

V. CONCLUSION

In this paper the concept of multipath routing protocol is implemented with selfish nodes detection. This paper illustrates that how the performance will be improved for the reliable data transmission by eliminating selfish nodes form communication path. For this purpose, the cluster based reputation scheme is proposed for the multipath routing protocol (AOMDV). Cluster based reputation technique for AOMDV routing protocol is able to provide reliable

communication and selects the best route based on the reputation value as decided by cluster head. The performance is evaluated on the basis of Data Packet Loss, Throughput and Average End to End Delay.

References

[1] Sarkar, Basavaraju and Puttamadappa, "Ad Hoc Mobile Wireless Networks: Principles, Protocols, and Applications", Auerbach Publications 2008.

[2] Rakesh Kumar Sahu, Rekha Saha, Narendra S. Chaudhari, "Fault Tolerant Reliable Multipath Routing Protocol for Ad hoc Network", Fourth International Conference on Computational Intelligence and Communication Networks, IEEE 978-0-7695-4850-0, pp. 117-121, 2012.

[3] Mina Vajed Khiavi , Shahram Jamali, **"**Performance Comparison of AODV and AOMDV Routing Protocols in Mobile Ad Hoc Networks", International Research Journal of Applied and Basic Sciences, ISSN 2251-838X / Vol, 4 (11), pp. 3277-3285, 2013.

[4] P.Periyasamy and Dr.E.Karthikeyan, "Performance Evaluation of AOMDV Protocol Based On Various Scenario And Traffic Patterns", International Journal of Computer Science, Engineering and Applications, Vol.1, No.6, pp. 33-48, December 2011.

[5] Santosh Kumar & Suveg Moudgil," Detection Of Selfish Node in DSR Based Manet Using Reputation Based Scheme", International Journal of Research in Engineering & Technology ISSN(E): 2321-8843; Vol. 2, Issue 8, Aug 2014, 1-10

[6] V.Preetha, Dr.K.Chitra, "Clustering & Cluster Head Selection Techniques in Mobile Adhoc Networks", International Journal of Innovative Research In Computer and Communication Engineering, Vol. 2, Issue 7, ISSN: 2320-9801, pp. 5151-5157, July 2014.

[7] Safaei, Zahra, Masoud Sabaei, and Fatemeh Torgheh. "An efficient reputation- based mechanism to enforce cooperation in MANETs." Application of Information and Communication Technologies, 2009. AICT 2009. International Conference on. IEEE, 2009.

[8] Marina MK, Das SR, "On-Demand multipath distance vector routing in ad hoc networks", Proceedings of the 9th IEEE International Conference on Network Protocols (ICNP), 2001.

[9] Ranjeet Kaur, Rajiv Mahajan, Amanpreet Singh, A Survey On Multipath Routing Protocols For Manets, International Journal of Emerging Trends and Technology in Computer Science, Volume 2, Issue 2, pp. 42-45, MarchApril 2013.

[10] Sangheethaa Sukumaran, Venkatesh. J, Arunkorath, A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks , International Journal of Information and Communication Technology Research, Volume 1 No. 2, pp. 73-80, June 2011.