Draft

A Novel Approach for Reliable Route Discovery in Mobile Ad-Hoc Network

*Shariq Mahmood Khan[1], R.Nilavalan[2], Abdulhafid Sallama[3]
Department of Electronic & Computer Engineering, Brunel University
London, United Kingdom
[1]shariq.khan@brunel.ac.uk
[2]rajagopal.nilavalan@brunel.ac.uk
[3]abdulhafid.sallama@brunel.ac.uk

Abstract — **AODV and DSR are normally taken as a standard in reactive routing protocols for Mobile Ad-hoc Network (MANETs). Both of these protocols are widely used in different applications of MANET because of their simple design and better performance. AODV does not provide optimal results in the scenarios where we have heavy traffic with large number of connections and higher routing load. In this paper, we have introduced a novel idea of "Reliability Factor" to determine reliable links between the intermediate nodes; based on this factor a reactive routing protocol is proposed, the simulation results of Reliability Factor Based Routing Protocol (RFBRP) show that it outperforms AODV and SP-AODV in terms of better packet delivery fraction, routing load and end-to-end delay**.

***Keywords* — AODV, Link Expiration Time, Reactive Routing, RFBRP, Route Reliability.**

I. Introduction

Mobile Ad-hoc Network (MANET) has been the focus of recent development in wireless communication paradigm. MANETs are becoming important day by day because of their applications in certain critical areas like military, disaster management, rescue operation etc. Interestingly, MANETs have several attractive features over conventional networks, like low cost, quick deployment and minimal configuration [1]. There is no fixed infrastructure in MANET and all communicating nodes are mobile, which results a dynamic topology. MANET consists of many mobile nodes where each node performs the role of a host as well as a router. Communication between two nodes takes place through intermediate nodes even if they are out of range, cf. Figure 1. The roaming of host nodes in any direction and with any speed causes frequent topology changes; therefore the node which wants to transmit data packet first needs to discover the route to the destination using one of the two types of route discovering protocols i.e. reactive (on demand) and proactive (table-driven) protocol.

There have been many table-driven routing protocols proposed for MANETs, such as destination-sequence distance-vector routing (DSDV) [2], wireless routing protocol (WRP) [3], cluster-head gateway switch routing (CGSR) [4], fisheye state routing (FSR) [5], and optimized link-state routing (OLSR) [6]. Similarly, there are various routing protocols based on reactive approach, like AODV [7], DSR [8] and ABR [9]. The performance of routing protocols depends upon the stability of links; breaking and reconstruction of links take major part of routing protocol task and during reconstruction of links data packets can be lost. Nodes periodically broadcast messages (Hello packets) to their neighbours in order to ensure their existence and to maintain the pre-established routes.

The AODV [7] routing protocol works on reactive approach for searching routes. The destination sequence number (DestSeqNum) identifies the most recent paths. DSR[8] is also an attractive protocol for routing in MANETs but it is different from AODV as it uses source routing, in which a data packet carries the complete path to be traversed. In AODV the source node and the intermediate nodes keep the next-hop information in order to transmit data packets from source to destination. In reactive routing protocols, the source nodes flood the RouteRequest packet to find an optimal route to the desired destination. Multiple routes are possibly discovered to different destinations as a result of single route request. Another important feature of AODV is that it uses a DestSeqNum to find fresh paths to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater or equal than the last DestSeqNum stored at the node with smaller hop-count.

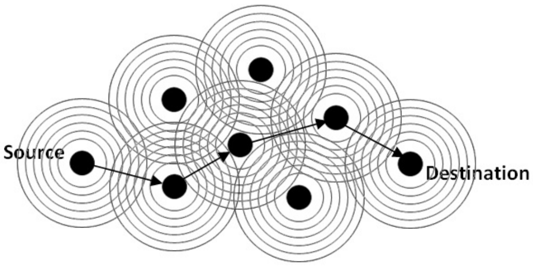


Figure 1. Mobile Ad-Hoc Network

A RouteRequest carries the source identifier (SrcID), the destination identifier (DestID), the source sequence number (SrcSeqNum), the destination sequence number (DestSeqNum), the broadcast identifier (BcastID), and the time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an

* *Research Scholar – Shariq Mahmood Khan is an assistant professor of computer science at NED University of Engineering & Technology.*

intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the DestSeqNum in the RouteRequest packet. If a RouteRequest is received multiple times, which is indicated by the (BcastID, SrcID) pair, the duplicate copies are discarded. All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send RouteReply packets to the source. Every intermediate node, while forwarding a RouteRequest, enters the previous node address and it's BcastID. A timer is used to delete this entry in case a RouteReply is not received before the timer expires. This helps in storing an active path at the intermediate node, as AODV does not employ source routing of data packets. When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

SP-AODV [10], is also a routing protocol based on AODV [7], which focuses on enhancing the performance of AODV. In this protocol authors presented a semi-proactive approach to find a route. The efficiency of this SP-AODV routing protocol mainly relies on the procedure updating some sections of the routing table by the nodes depending on the value of Counter field in the routing table. It employed Minimum Threshold (MinTH) and Maximum Threshold (MaxTH) values to control the Counter field in the routing table. The value MinTH is estimated as the 'number of neighbours of the node and MaxTH value is twice of the MinTH value.

This paper presents a routing protocol that reduces the routing overhead and selects a route between source and destination, which has minimum number of link breakage and hence increases the packet delivery ratio. A novel term "Reliability Factor (RF)" is introduced and an algorithm is proposed to discover a reliable route by using RF to select each link of the route having larger expiration time. In the rest of this paper, Section II explains the design and methodology of proposed protocol. Section III presents the simulation results and the discussion of the results. Section IV is devoted for conclusion and future research direction.

II. THE PROPOSED PROTOCOL RELIABILITY FACTOR BASED ROUTING PROTOCOL (RFBRP)

Our main objective is to improve the routing quality in MANET by using information available in the network and to select a stable routing path to reduce the routing overhead and packet loss. An algorithm has been designed based on reactive routing approach, which is normally adopted in MANET, such as AODV [7] and DSR [8]. We introduce a new factor to measure the reliability of a route called "Reliability Factor" (RF). It is found that RF plays an important role in selecting the reliable route.

A. Important Parameters

Let us first describe important parameters and notations, which have been used in this paper and then the route discovery phase of the proposed scheme, will be described.

1. **Link Expiration Time (LET):** The LET expresses the length of time for which two neighbours node in motion will remain connected. Suppose there are two nodes N_1 and N_2 having equal transmission ranges r. Let (x_1, y_1) and (x_2, y_2) be the x–y coordinates for nodes N_1 and N_2 respectively. As explained in [11] nodes N_1 and N_2 move at speeds of v_1 and v_2 at angles Θ_1 and Θ_2 respectively. Then the LET between nodes N_1 and N_2 is calculated using (1).

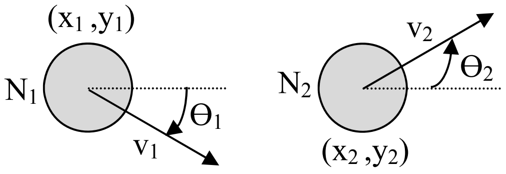


Figure 2. Link Expiration Time

$$\text{LET} = \frac{-(ab+cd)\pm\sqrt{(a^2+c^2)r^2-(ad-cb)^2}}{a^2+c^2} \quad (1)$$

Where

$a = v_1 \cos \Theta_1 - v_2 \cos\Theta_2$
$b = x_1 - x_2$
$c = v_1 \sin \Theta_1 - v_2 \sin \Theta_2$
$d = y_1 - y_2$

The parameters, mobility speed and direction information of equation 1 can be obtained from GPS or the node's own instruments and sensors.

2. **Route expiration time (RET):** The minimum value of the LET between the source and destination nodes is computed as equation (2).

$$\text{RET} = \min(\text{LET}_{rq} , \text{LET}_{\text{current Link}}) \quad (2)$$

3. **Hop Count (HC):** The total number of hops for a feasible path from source to destination.

4. **Reliability Factor (RF):** The difference of normalized values of Route Expiration Time (RET) and Hop Count (HC), which is calculated using equation (3).

$$\text{Reliability Factor (RF)} = \frac{\text{RET}}{\text{MaxRET}} - \frac{\text{HC}}{\text{MaxHC}} \quad (3)$$

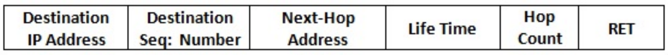
- **MaxRET:** It is the maximum value between the RET of route available in routing table and RET of the router request message and calculated using equation (4).

$$\text{MaxRET} = \text{Max}\ (\text{RET}_{rq}\ , \text{RET}_{rt}\ ) \qquad (4)$$

- **MaxHC:** It is the maximum value between the HC of route available in routing table and HC of the route request message and can be found as equation (5).

$$\text{MaxHC} = \text{Max}\ (\text{HC}_{rq}\ , \text{HC}_{rt}\ ) \qquad (5)$$

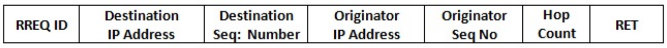
5. **Routing Table (RT):** Every node maintains the routing information in a table called routing table cf. Figure 3.



Destination IP Address	Destination Seq: Number	Next-Hop Address	Life Time	Hop Count	RET

Figure 3. Routing Table Structure

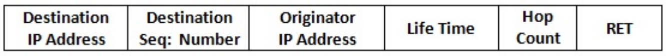
6. **Route Request (RREQ):** A packet initiated by a source or intermediate node to request a route toward the destination node cf. Figure 4.



RREQ ID	Destination IP Address	Destination Seq: Number	Originator IP Address	Originator Seq No	Hop Count	RET

Figure 4. Routing Request Packet Format

7. **Route Reply (RREP):** A packet initiated by a destination node in response to a route request cf. Figure 5.



Destination IP Address	Destination Seq: Number	Originator IP Address	Life Time	Hop Count	RET

Figure 5. Routing Request Packet Format

B. Route Discovery Phase

When a source node S needs a route to send a data packet to a specific destination node D but unable to find a route in its routing table, it broadcasts Route Request (RREQ) messages to all neighbouring nodes. The RREQ packet consists of RREQ ID, Destination IP Address, Destination Sequence Number, Originator IP Address, Originator Sequence Number, Hop Count and RET. The format of RREQ is described in Figure 4.

When a node receives a RREQ message it first creates a reverse route toward the source node if one is not already present. If there is already a route present in the table then it updates the existing route. Finding the reverse route is necessary for sending the reply packets back to the source node later on. If the receiving node is the destination node, it simply generates and sends back the Route Reply (RREP) message. The format of RREP packet is described in Figure 5.

If receiving node is an intermediate node and not the destination node D, and it already has a route in routing table towards the source node S, it calculates the RF of route in the routing table and RF of route in the RREQ message. If the RF of the RREQ message is higher than the RF of the route already present in the routing table, the new route is updated in the routing table. In case the RF value of RREQ message is less than zero, it drops this particular RREQ. It also selects the minimum value of Route Expiration Time (RET) between the current node and the RREQ sending node. Finally, the RREQ to the neighbours with minimum RET is broadcasted cf. Figure 6.

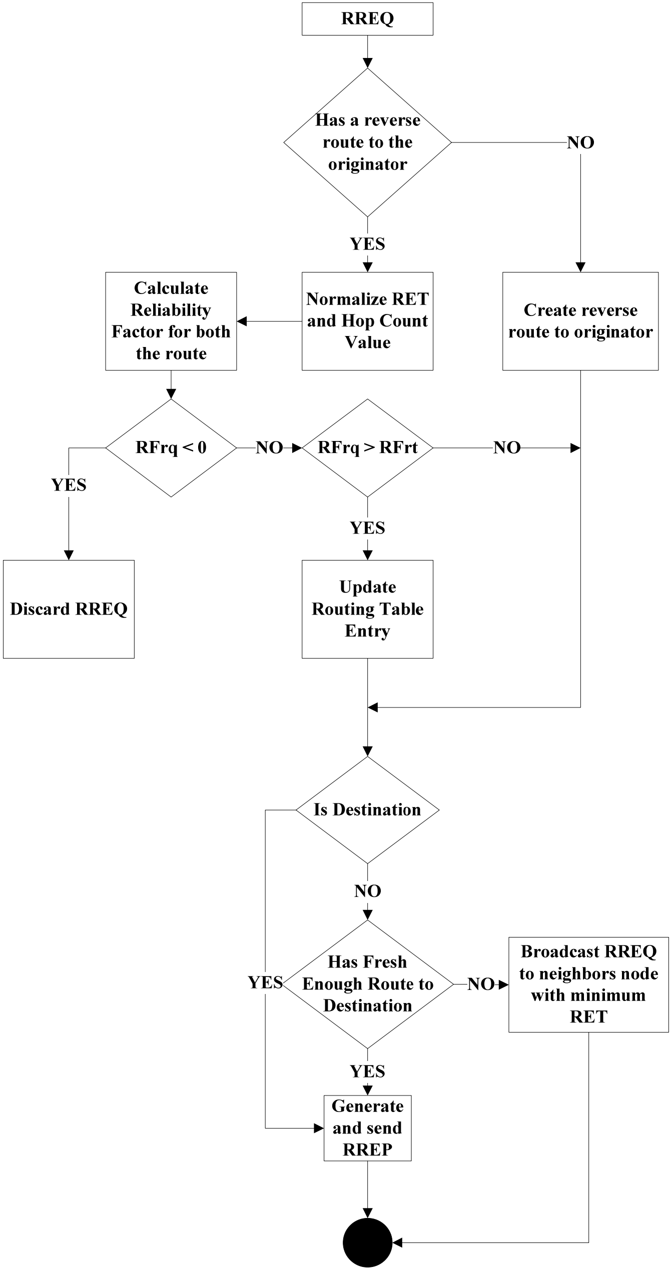

RREQ
Has a reverse route to the originator
NO
YES
Calculate Reliability Factor for both the route
Normalize RET and Hop Count Value
Create reverse route to originator
RFrq < 0
NO
RFrq > RFrt
NO
YES
YES
Discard RREQ
Update Routing Table Entry
Is Destination
NO
YES
Has Fresh Enough Route to Destination
NO
Broadcast RREQ to neighbors node with minimum RET
YES
Generate and send RREP

Figure 6. Routing Request Message Processing

A node generates a RREP message if it is either the destination node or an intermediate node having an active route to the destination. When a node receives a RREP message c.f. Figure 7 it first updates or creates a route from the previous hop toward the destination. If this node already has a route to the destination then it calculates the RF of the route, which is already present in the routing table and compares it to the RF of the RREP message. If the RF of the RREP message is greater than the RF of route already present in the routing table the route in the routing table is updated by the RREP message else the routing table is not updated and the RREP is then sent to the next hop towards the source node. If the RF value of RREP message is less than zero, it simply drops this particular RREP. If the receiving node is the originator it will send data packets to the destination through pre-determined route.

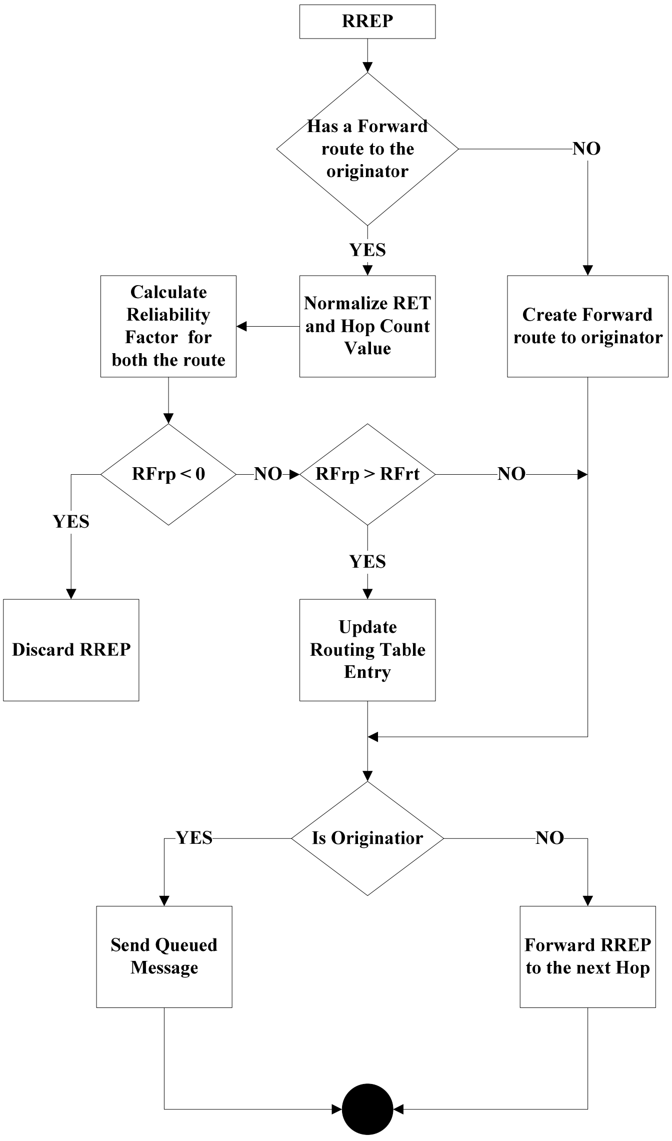

RREP
Has a Forward route to the originator
NO
YES
Calculate Reliability Factor for both the route
Normalize RET and Hop Count Value
Create Forward route to originator
RFrp < 0
NO
RFrp > RFrt
NO
YES
YES
Discard RREP
Update Routing Table Entry
YES
Is Originatior
NO
Send Queued Message
Forward RREP to the next Hop

Figure 7. Routing Reply Message Processing

III. Performance Evaluation

In order to evaluate the idea of using reliability factor for the selection of an optimal path, simulation of the proposed scheme is carried out using the Network Simulator (NS2.35) [12]. We use the Random Waypoint Mobility model [13], where each node independently chooses a random initial point and waits for a period called pause time. It then moves with a velocity chosen uniformly between minimum and maximum velocities to a randomly chosen destination. After reaching the destination, it waits again for the pause time and then moves to a new randomly chosen destination with a new chosen velocity. Each node repeats independently the above-mentioned movement until the simulation stops. Table 1 shows the simulation parameters.

TABLE I. Simulation Parameters

No of Nodes	50
Simulation Time	600 s
Area	1000m x 1000m
Speed	10 m/s
Maximum Connection	20,25,30,35,40,45,50,55,60
Traffic Type	Constant Bit Rate (CBR)
Data Packet Rate	4 pkt/s
Packet Size	512 Bytes

Simulation of the proposed scheme is performed with 50 nodes, which is enough to evaluate the required parameters in the area of 1000 x 1000 meters. This setting provides enough space for the mobility of nodes and to check the discovery of new routes. The simulation is run on different number of maximum connection or traffic load, which is enough to verify that the proposed scheme is worth to implement in the scenario where more overhead is expected.

A. Performance Parameters

Following metrics are used in varying scenarios to evaluate the proposed protocols.

1. **Control Packets Overhead:** During the simulation time the total number of routing packets sent out is considered as control packets overhead.

2. **Packet delivery Fraction:** This is defined as the ratio of the number of data packets received by the destinations to those sent by the CBR sources.

3. **Average end-to-end delay**: It is defined as the delay between the time at which the data packet was originated at the source and the time it reaches the destination. Data packets that get lost en route are not considered. Delays

due to route discovery, queuing and retransmissions are included in the delay metric.

The performance of the proposed algorithm is compared with traditional AODV [7] and recently proposed SP-AODV [10] in terms of control packet overhead, network packet delivery ratio and Average End-to-End Delay. The proposed algorithm RFBRP outperforms AODV and SP-AODV protocol in term of overhead, packet delivery and end-to-end delay.

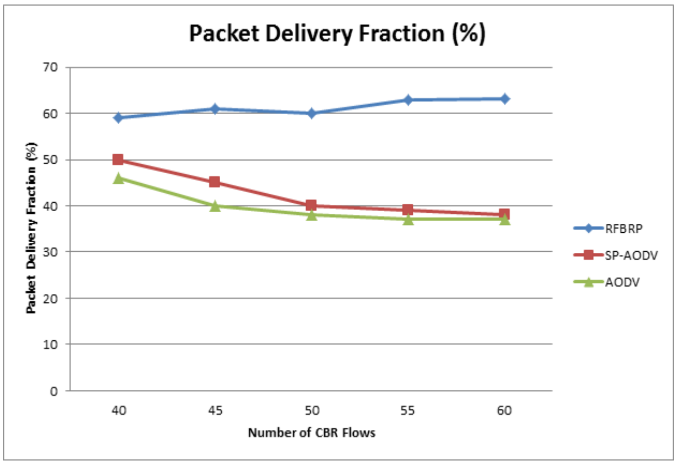


Figure 8. Packet Delivery Ratio vs. Number of CBR Flows

Figure 8 shows the advantage of the proposed protocol in terms of packet delivery fraction (PDF) with varying traffic load. As the traffic load increases we can see that AODV and SP-AODV protocols decreased the packet delivery fraction, because of the increase in the number of routing and data packet. This increase in routing and data packets caused channel contention and packet collision that leads to drop in packet delivery. Figure 8 also shows that RFBRP outperforms AODV and SP-AODV at every traffic load. This PDF improvement of RFBRP is due to the selection of route with longest expiration time as well as the reduction of control packets. The less rebroadcast of routing message causes smaller bandwidth consumption. This also effect positively on the network and reduces collisions and contentions, and eventually gives the higher packet delivery. When traffic load is 40 CBR flows, RFBRP enhances around 10% and 15% PDF as compare to SP-AODV and AODV respectively .On the high traffic load PDF enhancement of RFBRP is around 20%.

Number of routing packets with respect to traffic load is shown in Figure 9.As the traffic load increases in the network the routing packets increases gradually for AODV and SP-AODV protocols. Basically, increasing traffic load increases the redundant re transmission of the routing packets, causing congestion and packet collision in the network, as a result more RREQ packets and data packets are dropped before reaching the destination. This triggers new route discovery process that causes more routing packets in the network. The proposed protocol has less routing packets than AODV and SP-AODV because RFBRP controls the redundant retransmission of the RREQ packets by dropping the redundant broadcast packets and also it selects the reliable route between source and destination. The selection of reliable route reduces the route failures. Hence, the frequent route discovery is avoided and which in turn reduces the routing load in the route discovery process. RFBRP yields a significant improvement in term of routing overhead as compare to AODV and SP-AODV.

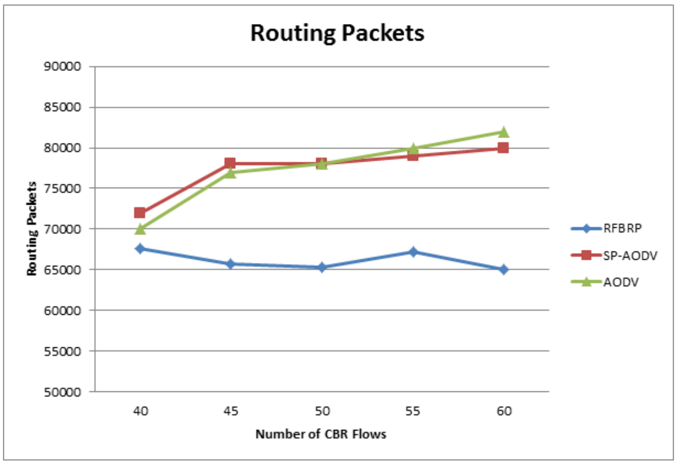


Figure 9. Network Routing Load vs. Number of CBR Flows

The Average End-to-End delay is illustrated in Figure 10 against the traffic load. As the traffic load increased the end-to-end delay of both protocols increases. Because of the selection of the reliable and shorter route, the RFBRP has resulted in less amount of time on average to transfer data packets as compared to AODV and SP-AODV.

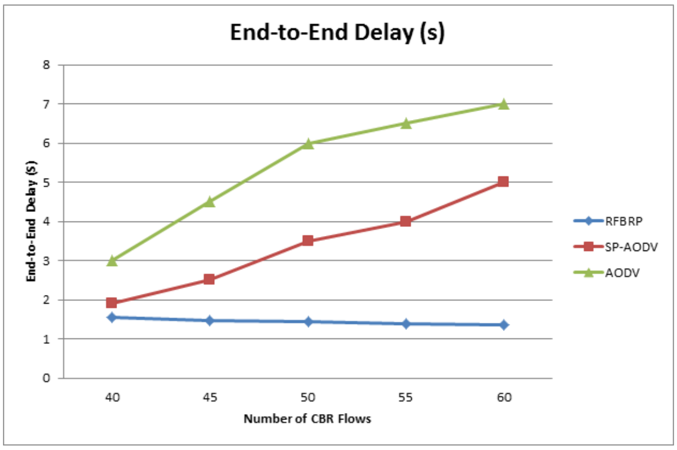


Figure 10. End-to-End delay vs. Number of CBR Flows

IV. CONCLUSION

In this paper a new route discovery mechanism has been presented which decides the optimal route on the basis of Reliability Factor. The proposed route discovery process considers Reliability Factor as the primary metric, while selecting the route, which minimizes the routing failure and in turn reduces the number of route discovery requests as well as the computation overhead of every node involved in route discovery process. Consequently, the overall performance of the routing protocol improves. The important contribution of this paper is the design and development of novel route discovery process based on Reliability Factor in a reactive routing protocol. Future work will focus on the further optimization of the proposed metric and comparison with regard to other existing routing protocols used for MANET.

References

[1] N. Meghanathan, "Survey and taxonomy of unicast routing protocols for mobile ad hoc networks," *The International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks,* vol. 1, pp. 1-21, 2009.

[2] C. E. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in *ACM SIGCOMM Computer Communication Review,* 1994, pp. 234-244.

[3] S. Murthy and J. Garcia-Luna-Aceves, "A routing protocol for packet radio networks," in *Proceedings of the 1st Annual International Conference on Mobile Computing and Networking,* 1995, pp. 86-95.

[4] S. Murthy and J. J. Garcia-Luna-Aceves, "An efficient routing protocol for wireless networks," *Mobile Networks and Applications,* vol. 1, pp. 183-197, 1996.

[5] G. Pei, M. Gerla and T. Chen, "Fisheye state routing: A routing scheme for ad hoc wireless networks," in *Communications, 2000. ICC 2000. 2000 IEEE International Conference On,* 2000, pp. 70-74.

[6] T. Clausen, P. Jacquet, C. Adjih, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum and L. Viennot, "Optimized link state routing protocol (OLSR)," 2003.

[7] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Mobile Computing Systems and Applications, 1999. Proceedings. WMCSA'99. Second IEEE Workshop On,* 1999, pp. 90-100.

[8] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," in *Mobile Computing*Anonymous Springer, 1996, pp. 153-181.

[9] C. Toh, "Associativity-based routing for ad hoc mobile networks," *Wireless Personal Communications,* vol. 4, pp. 103-139, 1997.

[10] T. Dargahi, A. M. Rahmani and A. Khademzadeh, "SP-AODV: A semi-proactive AODV routing protocol for wireless networks," in *Advanced Computer Theory and Engineering, 2008. ICACTE'08. International Conference On,* 2008, pp. 613-617.

[11] W. Su, S. Lee and M. Gerla, "Mobility prediction and routing in ad hoc wireless networks," *International Journal of Network Management,* vol. 11, pp. 3-30, 2001.

[12] K. Fall and K. Varadhan, "The network simulator (ns-2)," *URL: Http://Www.Isi.Edu/Nsnam/Ns,* Retrieved in 2012.

[13] W. Navidi and T. Camp, "Stationary distributions for the random waypoint mobility model," *Mobile Computing, IEEE Transactions On,* vol. 3, pp. 99-108, 2004.