Multipath Node-Disjoint Routing with Backup List Based on the AODV Protocol

Vahid Zangeneh[i] and Shahriar Mohammadi[ii *]

ABSTRACT

In recent years, routing has been the most focused area in ad hoc networks research. On-demand routing in particular, is widely developed in bandwidth constrained mobile wireless ad hoc networks because of its effectiveness and efficiency. Most proposed on-demand routing protocols are built and relied on single route for each data session. Whenever there is a link disconnection on the active route, the routing protocol must perform a route recovery process. Meanwhile, AODV (Ad Hoc On-demand Multipath Distance Vector) creates single-path route between pairs of source and destination nodes. This paper proposes a new approach of multipath node-disjoint routing based on the AODV protocol which creates two paths from a source node to a destination node without any common nodes. Furthermore, in this research, NS-2 simulator is used to produce simulations of both AODV and the proposed method. At the end, the results of the two simulations are compared to validate the effectiveness and performance of proposed method.

KEYWORDS

Routing, Node-disjoint, Multipath, AODV, On-demand

1. INTRODUCTION

A mobile ad hoc network (MANET) is a type of wireless network that is composed of wireless mobile nodes. Each mobile node dynamically changes the network topology without relying on any wired backbone network or fixed base station. Mobile nodes in MANETs are constrained by their limited power, processing, memory resources and high degree of mobility. In such networks, the wireless mobile nodes may dynamically join or leave the network topology. In MANETs, many routing protocols have been suggested [1]-[2] to make communications among mobile nodes.

In conventional wired networks, nodes do not change the network topology frequently. Routing protocols in wired networks are inadequate for ad hoc networks where the network topology changes dynamically. In a network composed of mobile nodes changes in the network topology require frequent rebuilding of routes. Therefore, maintaining stable routes may be infeasible. Consequently, routing protocols for MANETs consider node mobility, stability and the reliability of data transmission. Based on these criteria, various multipath routing protocols have been suggested as extensions to conventional single-path routing protocols AODV [3]-[4]. For example, the Ad Hoc On-demand Multiple Distance Vector (AOMDV [5]) protocol discovers multiple routes by recording the path over which RREQ packets have been sent. Ad Hoc On-demand Distance Vector Backup Route (AODV-BR [6]), a node-disjoint multipath routing protocol based on AODV in mobile ad hoc networks (MP-AODV [7]) and AODV-Multipath (AODVM [8]) protocols use overhearing to send RREP packets for discovering multipath routes. In addition, an interference avoidance multipath routing protocol based on greedy forwarding in MANETs (GIMR [9]) uses greedy forwarding.

In this paper, a new node-disjoint multipath routing algorithm based on the AODV protocol for MANETs is suggested. This method improves the packet transmission rate and reduces the end-to-end delay by utilizing the main and backup routes that are node-disjoint. The reminder of the paper is organized as follows. Section 2 reviews the related studies. In Section 3, we describe the proposed method (MNL-AODV). Section 4 compares the MNL-AODV performance with AODV by using NS-2 simulator.

2. RELATED STUDIES

Multipath routing establishes multipath routes between source and destination nodes. For the fault tolerance purpose, even if one route failure occurs, source nodes can maintain connections by using other routes. So, using multipath routing protocols can reduce data transmission failures and delay times that are caused by route disconnection.

i V. Zangeneh is with the Department of Information Technology, K.N.Toosi University of Technology, Tehran, Iran (e-mail: vz.vahidzangeneh@gmail.com).

ii * Corresponding Author, S. Mohammadi is with the Department of Information Technology, K.N.Toosi University of Technology, Tehran, Iran (e-mail: mohammadi@kntu.ac.ir).

Multipath routing protocols search node-disjoint, link-disjoint or non-disjoint routes during the route discovery process. Node-disjoint routes have no node or link in common, while Link-disjoint routes though have no link in common may have some nodes in common [10]. Non-disjoint routes may use nodes or links in common. In non-disjoint or link-disjoint multipath routes when a common node or link fails, main route and backup routes will be disconnected at the same time. However, in node-disjoint routes, main routes and backup routes use completely different nodes or links. Therefore, even though main route becomes disconnected, data transmission is continued through the backup route.

The AODV protocol is known as a pure on-demand routing protocol because a mobile node does not have to maintain any routing information if it is not located in an active path. The AODV protocol contains a route discovery and a route maintenance mechanism. To detect a fresh route from a stale one, each node maintains two counters called node sequence number and broadcast ID. Each route request packet (RREQ) contains information about the destination sequence number and the source sequence number as well as source address and destination address. The sequence numbers are used to indicate the route freshness. Each neighboring node either sends a reply (RREP) to a source or rebroadcasts a request message to its neighbors depending on whether it is the destination or not. If a node is not the destination, it needs to keep track of a request packet to setup a reverse path as well as a forward path. When a destination replies back to a source, it uses the reverse path. Mobile nodes can determine whether a route is a current one or as a tale one by comparing the destination sequence number in the route request packet with that of the sequence number stored in the routing table. If the route request sequence number is greater than the recorded one, it does not send any reply to the source. Instead, it rebroadcasts the request message. An intermediate node replies if the route request sequence number is less than or equal to the sequence number stored in the routing table. If a node has a current route, it sends a reply using a unicast route reply packet. The reply packet travels along the reverse path which has been previously set up. When a reply packet travels back through the reverse path, each intermediate node sets up a forward pointer to the node from which it receives this reply. When a route reply packet reaches the source, the source starts sending data packets to the destination using the discovered path. If that source learns more routes later, it updates its routing table accordingly.

The AOMDV protocol establishes loop-free link-disjoint paths in the network. When intermediate nodes receive RREQ packets from the source node, AOMDV stores all RREQ packets, unlike the conventional AODV protocol which discards duplicates. Hence, each node maintains a firsthop-list whose information is from an additional field called firsthop in RREQ packet to indicate the neighbor node of the source node. If firsthop of the received RREQ packet is duplicated from its own firsthop-list, the RREQ packet is discarded. On the other hand, the RREQ packet is not duplicated from the previous RREQ packets. Then, the node updates the nexthop, hopcount and advertised-hopcount in routing table. At the destination, RREP packets are sent from each received RREQ packet. The multipath routes are made by RREP packets following the reverse routes that have been already setup in the intermediate nodes.

For the AODVM protocol, intermediate nodes are not allowed to send a RREP packet directly to the source node. The intermediate nodes do not further discard the duplicate RREQ packets; however, they record all the received RREQ packets in the routing table. The destination node sends one RREP for all the received RREQ packets. An intermediate node forwards the received RREP packet to the neighbor in the routing table. Whenever a node overhears one of its neighbors broadcasting RREP packet, removes that neighbor from its routing table because they are not allowed to participate in more than one route.

For the AODV-BR protocol, neighboring nodes overhear the RREP packets for establishing and maintaining the backup routes during the route initiation process. If any part of the main route is broken, nodes broadcast error packets to the neighboring nodes. When neighboring nodes receive the error packet, they establish an alternate route using information about the previous overheard RREP packets.

AOMDV has the overhead of storing multipath next hops and hop counts and the first hop list for each destination. By overhearing the packets broadcasted by neighbors, AODVM might not establish alternate routes depending on the path along which the RREP packets are sent. Moreover, to speak strictly, AODV-BR is not a multipath routing protocol because it only maintains bypass routes around the main routes.

MP-AODV protocol uses the modified RREQ and RREP packets that have additional 1bit flag of 'F'. This flag distinguishes the packets into the main route or backup route discovery processes. Unlike the conventional AODV, intermediate nodes that receive the RREP packet increase the RREQ ID value in the routing table. By increasing the RREQ ID value, the protocol ensures that a backup route will not use any nodes that belong to the main route. When a source node receives the RREP packet, the main route is established. Then the source node starts data transmission and broadcasts the RREQ_2 packet. The RREQ_2 is a packet with a RREQ ID value of two and its flag 'F' is set to one. When the RREQ_2 packets are delivered to the intermediate nodes, the RREQ ID values in the routing table are compared with the RREQ ID values in the RREQ_2 packets. If they are

identical, the nodes discard the RREQ_2 packets. If not, the nodes forward the RREQ_2 packets continuously. When nodes belonging to the main route receive the RREP packet, the RREQ ID value in the RREQ_2 packet and the RREQ ID value in the routing table become identical because the protocol has already increased the RREQ ID value in the routing table during the previous route discovery process. After this process, the intermediate nodes belonging to the main route will not join the backup routes.

3. PROPOSED METHOD

In this paper, the MNL-AODV (Multipath Node-disjoint with backup List AODV) algorithm based on AODV protocol is proposed. This algorithm uses two node-disjoint routes between source and destination pairs. MNL-AODV reduces the transmission delay using backup route when the main route is broken while the backup route is stable.

A. Changes of AODV Routing Table

In the suggested algorithm by this research, the source node maintains two node-disjoint paths to each destination. Thus, the AODV routing table must be changed. We modified the AODV routing table so that a route entry is able to maintain information of the main and the backup routes (see Table 1).

B. Changes of AODV Packet

Two new fields of a flag 'F' (of one bit) and a Backup_List are two extra fields that are added to the RREQ packet shown in Table 2. When intermediate nodes receive the RREQ packet, they rebroadcast or drop it depending on the provided information by both the RREQ's flag 'F' value and Backup_List. The MNL-AODV algorithm uses the flag 'F' to distinguish between the main route and backup route discovery processes. During the main route discovery process intermediate nodes belonging to the main route are stored in the RREQ's Backup_List. The Backup route discovery process does not involve nodes which are previously stored in the Backup_List.

TABLE 1
THE MNL-AODV ROUTING TABLE

Destination IP Address
Sequence Number
Next Hop (main route)
Hop Count of Next Hop (main route)
Expiration Timeout (main route)
Next Hop (backup route)
Hop Count of Next Hop (backup route)
Expiration Timeout (backup route)

TABLE 2
THE MNL-AODV RREQ PACKET

Type	J	R	…	D	**F**	Reserved	Hop Count
RREQ ID							
Destination IP Address							
Destination Sequence Number							
Originator IP Address							
Originator Sequence Number							
Backup_List							

C. Route Discovery

When a source node wants to communicate with a destination node while there is no path to the destination node in the routing table, it broadcasts the RREQ packet with an 'F' flag value of zero to initiate the main route discovery process. When an intermediate node receives the RREQ packet with the 'F' flag value of zero which is not the destination determined in the RREQ packet, it acts as follows: (1) creates the reverse pointer to the node from which RREQ comes and records it as a reverse path, (2) updates the routing table similar to the conventional AODV protocol, (3) inserts its IP address into the RREQ's Backup_List, (4) rebroadcasts RREQ.

If the destination node receives the RREQ packet, it acts as follows: (a) sends the RREP to the source node for establishing the forward path (as a main route), (b) creates a new RREQ packet with 'F'=1 and 'D'=1, (c) copiest the Backup_List of the received RREQ into the new RREQ packet's Backup_List, (d) broadcasts the new RREQ packet to the source node to initiate the backup route discovery process. Then each next received RREQ packet at the destination is discarded. The backup route discovery process creates the reverse path from the source node to the destination node that will be considered as a backup route in the source node.

When a source node receives the RREP packet, the main route is established and the source node starts data transmission. If the source node receives a RREQ packet with an 'F' flag value of one, it inserts the reverse path as a backup route into the routing table and sends a RREP packet to the destination node. When the destination node receives the RREP packet, it drops it.

When an intermediate node receives the RREQ packet with an 'F' flag value of one, it compares its IP address with the IP addresses in the RREQ's Backup_List. If a match is found, it means that the current node belongs to the main route and cannot be a member of the backup route. Therefore, it discards the RREQ packet. If a match case is not found, it records the reverse path as a backup route to the destination node and behaves similar to the conventional AODV protocol.

As it is shown in Fig. 1, since node S needs to send data to the node D but it has no path in the routing table; it

initiates the route discovery process by broadcasting a RREQ packet with 'F' flag value of zero. Node M receives the RREQ packet and creates a reverse path to node S and inserts its IP address into the RREQ's Backup_List and rebroadcasts RREQ. Node N as a neighbor of node M receives the RREQ packet and creates the reverse path to M, and adds its IP address to the Backup_List and rebroadcasts RREQ. When node D receives RREQ, the Backup_List includes {N, M} nodes as the members of the main route. The other nodes such as K or P might receive the RREQ packet, assuming that AODV selects {S, M, N, and D} as a route from S to D.

According to Fig. 2, when the destination node D receives the RREQ packet with an 'F' flag value of zero, it sends a RREP packet to node S by using the created reverse path and creates a new RREQ with 'F' flag value of one. Then copies the Backup_List ({M, N}) of the received RREQ into the new RREQ packet's Backup_List and sends it towards the node S which is determined as the source node address in the received RREQ packet. When nodes N and M as members of the main route receive RREQ with the 'F' flag value of one discard it, because they detect their addresses in the Backup_List. When nodes such as P and K that are not involved in the main route receive RREQ with 'F' flag value of one, create reverse pointer to the node from which the RREQ came and record it as a main route to the destination node D. When node S receives RREQ with 'F' flag value of one, it records the reverse path in the routing table as a backup route.

According to the conventional AOVD**,** when 'D' flag in the RREQ packet is set to one, it indicates that only the destination can respond to this RREQ by sending back a RREP packet to the source node.

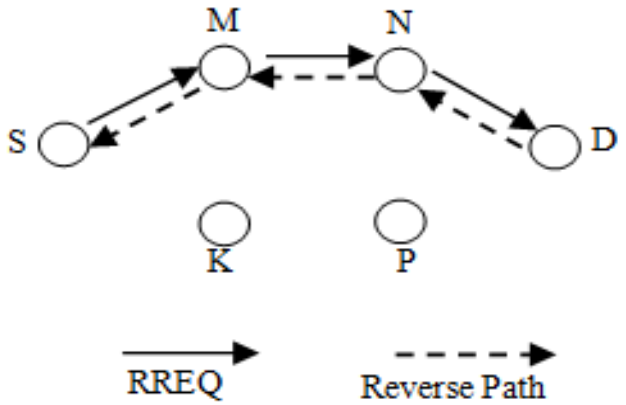

Figure 1: The Main Route Discovery Process

As we mentioned, the 'D' flag of RREQ packet that is broadcasted by the destination node to make the backup route is set to one. Fig. 3 illustrates the route discovery process with the following assumptions:
Des-IP: Destination IP Address in the received packet
My-IP: The current node's IP Address.

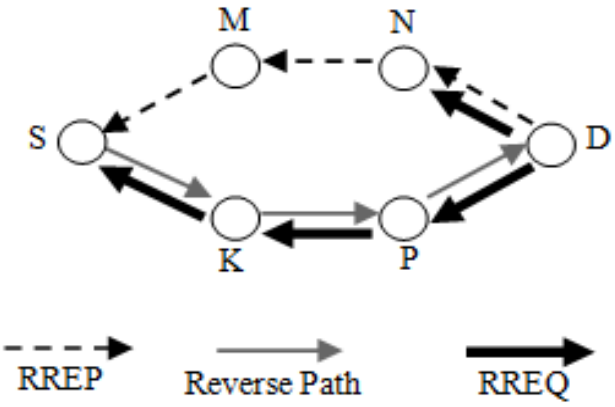

Figure 2: The Backup Route Discovery Process

Input: RREQ packet with 'F' flag
IF (packet's 'F' == 0)
{
  if (packet's Des-IP ≠ My-IP) // intermediate
  {
    • Insert My-IP into Backup_List
    • Conventional AODV algorithm is used
  }
  else // destination
  {
    •Send a RREP for received RREQ
    •Create RREQ with 'F'=1, 'D'=1
    •Copy Backup_List into the created RREQ
    •Send the created RREQ to source
  }
}
ELSE **//F=1**
{
  if (packet's Des-IP == My-IP) // source
  {
    •Record reverse path as a backup route
    •Send RREP to destination node
  }
  else if (My-IP ϵ Backup_List) //intermediate
  {
    •Discard RREQ packet.
  }
  else
  {
    • Conventional AODV algorithm is used
    • Record reverse path as a route to destination
  }
}

Input: RREP packet
IF (packet's Des-IP == My-IP)
{
  If (there is data to send)
  {
    • Discard RREP.
    • Send data.
  }
  else
  {
    • Discard RREP.
  }
}
Else { • Conventional AODV algorithm is used.}

Figure 3: The MNL-AODV Route Discovery process

D. Route Maintenance

In general, route links in ad hoc networks are broken frequently due to mobility of nodes, congestion and packet collisions. Each node of MNL-AODV depends on sending out HELLO packets to maintain local connectivity like AODV. Route maintenance in MNL-AODV is a simple extension of AODV route maintenance. MNL-AODV also uses RERR packets like AODV. Failure to receive a HELLO packet from a neighbor is regarded as an indication that the link to the neighbor is broken. A RERR packet is propagated from the upstream node of the link failure to the source node. When an intermediate node receives a RERR packet, it marks its route invalid to the destination. Then it propagates the RERR to its precursor node along the reverse path. After receiving RERR, the source invalidates the route to destination and chooses valid node-disjoint backup route as an active path from the routing table or initiates a new route discovery when no backup routes are available to continue forwarding data packets.

4. PERFORMANCE EVALUATION

We evaluated the effectiveness of MNL_AODV relative to AODV using NS-2 simulator [11]. A simulated field is 1000m × 1000m and simulations are performed for 1000 seconds. Each node moves at random times with random directions. The distributed coordination function (DCF) of IEEE 802.11 [12] for wireless LANs is used as the MAC layer protocol with a 250m transmission radius. The packet size is set to 500 byte and sending rate is 3 packets per second. Traffic pattern consists of 10 CBR/TCP connections which are randomly selected between source-destination pairs. This set of results consists of 50 mobile nodes.

A. Performance Metrics

We consider the following performance metrics:

- *Packet Delivery Ratio*: The ratio between the number of received packets by the destination and the number of sent packets by the source.
- *Average Delay*: The mean time taken by the data packets to reach their destinations.
- *Routing Load Percentage*: The ratio between the total size of control packets and the total size of data and control packets.
- *Routing Overhead*: The total size of routing packets per second.
- *Route Discovery Frequency*: The number of route discovery process per second.
- *Route Discovery Overhead*: The number of route discovery packets per second.

B. Simulation Results

Figures 4 to 9 show the results with varying node speeds. The routes reliability is reduced by increasing speed of the nodes. Thus, in this situation backup routes can improve the performance of the algorithm. In Fig. 4, packet delivery ratio of these two protocols is shown. This figure shows the packet delivery ratio of MNL-AODV is higher than AODV. By increasing the speed of nodes, this metric is decreased. Although Fig. 4 shows that the delivery ratio of both of algorithms decreases but the average decrement of delivery ratio of MNL-AODV is 3% lower than that of AODV. As shown in Fig. 5, the average delay of MNL-AODV is lower than that of AODV by about 30% because when the main route is broken, MNL-AODV switches to backup route while AODV reinitiates the route discovery process. The MNL-AODV by initiation of route discovery process can obtain two routes and uses these routes to send data to a destination. Thus, the MNL-AODV's routing load percentage is less than that of AODV by about 20% as shown in Fig. 6. The total size of routing packets per second which is routing overhead is shown in Fig. 7. This figure shows that the MNL-AODV's routing overhead is less than that of AODV. The illustration of Fig. 8 shows that the performance of the node-disjoint multipath routing protocols (i.e. MNL-AODV) at the point of the route discovery frequency is better than that of a single path routing (i.e. AODV).

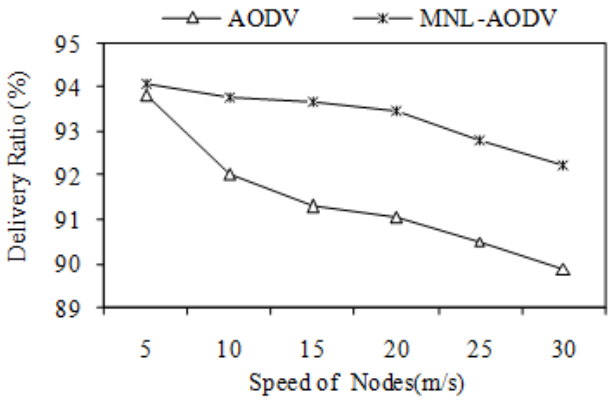

Figure 4: Delivery Ratio

As shown in Fig. 8, the average route discovery frequency of MNL-AODV is lower than that of AODV about 25%. According to Fig. 9, it is realized that the route discovery overhead of MNL-AODV is lower than that of AODV by about 26%.

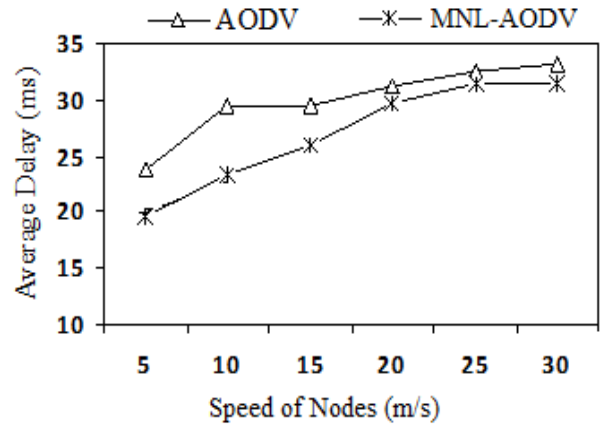

Figure 5: Average Delay (millisecond)

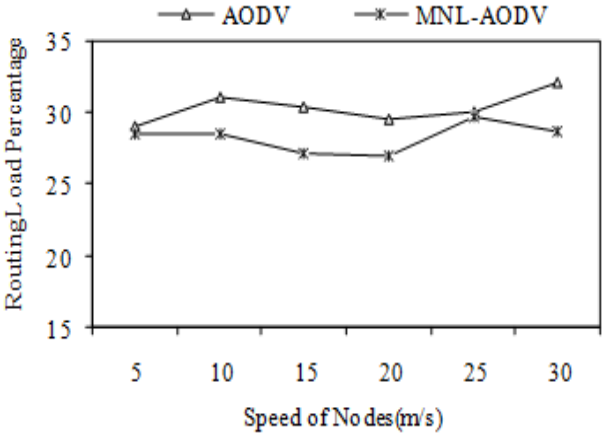

Figure 6: Routing Load Percentage

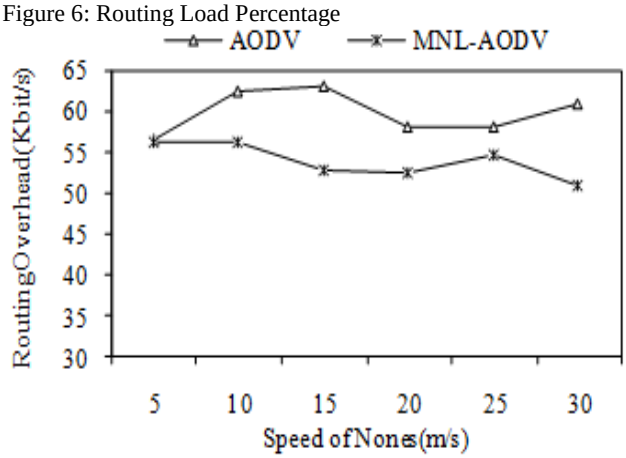

Figure 7: Routing Overhead (kilo bit per second)

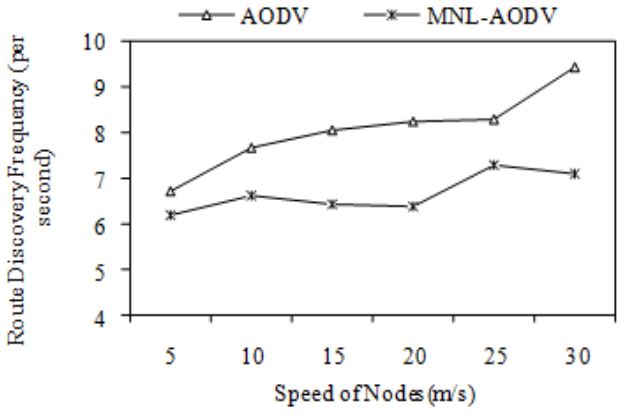

Figure 8: Route Discovery Frequency (per second)

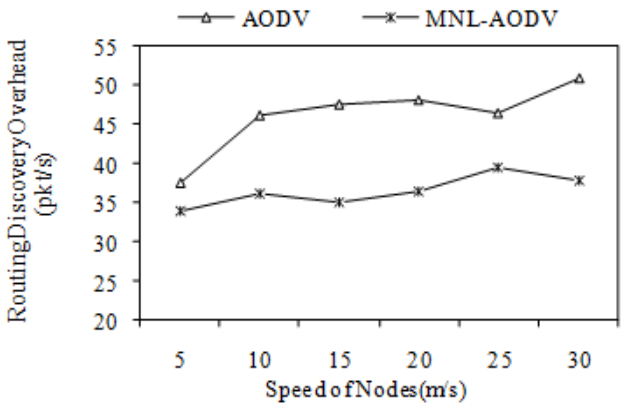

Figure 9: Routing Discovery Overhead (packet per second)

5. REFERENCES

[1] M. Tarique, E. Tepe, S. Adibi and S. Erfani, " Survey of multipath routing protocols for mobile ad hoc networks", Journal of Network and Computer Applications, Elsevier , 2009, pp.1125-1143.

[2] A. Boukerche, B. Turgut, N. Aydin, Z Mohammad, A. Ladislau Boloni and D. Turgut, "Routing protocols in ad hoc networks: A survey" Journal of Computer Networks, Elsevier, 2010, pp.3032-3080.

[3] CE. Perkins and EM. Royer, "Ad hoc On-Demand Distance Vector Routing", In Proc. of IEEE Workshop on Mobile Computing Systems and Applications, February, 1999.

[4] RFC3561: Ad hoc On-Demand Distance Vector (AODV) Routing.

[5] M. K. Marina and S. R. Das, "On-demand Multiple Distance Vector Routing in Ad Hoc Networks", Proceedings of the International Conference for Network Protocol, 2001.

[6] Sung-Ju Lee and Mario Gerla, "AODV-BR: Backup Routing in Ad hoc Networks", Wireless Communications and Networking Conference, 2000.

[7] C. Ahn, S. H. Chung, T. H. Kim and S. Y. Kang, "A Node-Disjoint Multipath Routing Protocol Based on AODV in Mobile Ad-hoc Networks", International Conference on Information Technology, IEEE, 2010.

[8] Z. Ye, SV. Krishnamurthy and SK. Tripathi, "A framework for reliable routing in mobile ad hoc networks", In Proc. of the 22th annual joint conference of the IEEE computer and communications societies (INFOCOM), vol.1, 2003, pp.80-270.

[9] W. Yang, X. Yang, G. Liu and W. Yu, "An Interference Avoidance Multipath Routing Protocol based on Greedy Forwarding in MANETs", IEEE, 2010.

[10] M.T.Toussaint, "Multipath Routing in Mobile Ad Hoc Networks", TU-Delft/TNO Traineeship Report.

[11] K. Fall and K. Varadhan, "The ns manual". Available: http://www.isi.edu/nsnam/ns/ns-do-cumentation.html.

[12] IEEE Std. 802.11.Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, 1999.