Journal of Engineering Sciences, Assiut University, Vol. 34, No. 3, pp. 843-857, May 2006

COMPARATIVE EVALUATION OF MOBILE AD HOC NETWORK (MANET) PROTOCOLS ROUTING

M. K. Ahmed ; O. El-Ghandour and H. Ramadan
Helwan University, Electronics & Communications and Computer Engineering Department, Cairo, Egypt.
e-mail:osamaghn@hotmail.com
e-mail:prof-MK@hotmail.com :
e-mail:hedia_ramadan@yahoo.com

(Received February 27, 2006 Accepted April 20, 2006)

ABSTRACT– *Wireless Ad Hoc networks are relatively new and are gaining ground in research due to promises they offer. Wireless Ad hoc networks do not require predefined configuration and have no fixed infrastructure. They are self-organizing and self-configuring networks. Several protocols have been developed that vary in the performance and complexity. Most routing protocols for mobile ad hoc networks, such as: Ad Hoc On Demand Distance Vector Protocol (AODV), Dynamic Source Routing (DSR) are designed without explicity considering quality of service of the generated route. These routing protocols provide the capability for establishing minimum hop paths between nodes on a best effort basis regardless of QoS. In our work, we analyze the performance of these protocols and we present an efficient scheme for support QoS over MANET named Hierarchical Dynamic Source Routing protocol (HDSR). The performance aspects we study are fraction of routing overhead, end-to-end delay and throughput. It was shown via computer simulations that (HDSR) improves these performance aspects in wireless mobile ad hoc networks compare to other protocols.*

KEYWORDS: *Ad hoc, AODV, DSR, HDSR, QoS.*

1. INTRODUCTION

Mobile ad hoc networking is becoming increasingly popular as a mean of providing instant networking to groups that may be within the transmission range of one another. These networks are self-initializing, self-configuring, and self-maintaining, all of which can be coined with term "self-organizing". Since connectivity changes constantly (**Fig. 1**), a major challenge in mobile ad hoc network environments is a reliable and efficient routing service. Each node in the network acts as a router, forwarding data packets for other nodes. So, Routing is an essential part of network protocols to provide self-organizing capability, and it is the most widely studied element for ad hoc networks. A central challenge in the design of ad hoc networks is the development of dynamic routing protocols that can efficiently find routes between

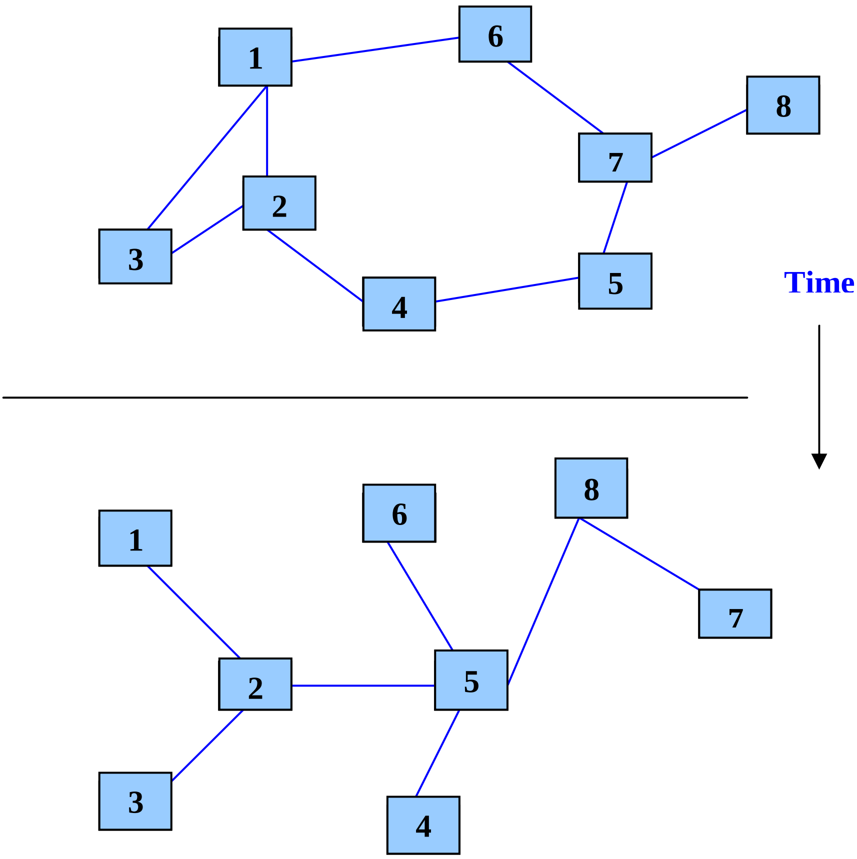


Fig. 1: Ad-Hoc Mobile Networks. Connectivity changes as nodes move.

two communicating nodes. The routing protocol must be able to keep up with the high degree of node mobility that often changes the network topology drastically and unpredictably.

Various constraints are introduced by the Ad hoc networks:

– ***Dynamic topology***: which evolves very quickly because each node can move arbitrarily and disappear randomly without any notification. From where need for routing mechanism which adapts with the nodes connectivity at a given moment.

– ***Radio channel of communication***: indeed the connections are with variable rates and limited bandwidth.

– ***Nodes function with batteries***: a reduced autonomy in term of energy. Moreover each node serves as a host as well as a router and uses consequently its own energy to route flows intended for other nodes of the networks.

– ***Limited security***: since ad hoc networks are more vulnerable to physical security threats, provisions for security must be made.

The ability to provide an adaptive quality of service (QoS) in such a mobile environment is a key to the success of next generation wireless communications systems. Recently there has been a considerable amount of QoS research. However, the main part of this research has been in the context of framework components, and much less progress has been made in addressing the issue of a group management to provide QoS within an ad hoc network.

1.1. Ad Hoc Routing Protocols Overview

Below we present an overview of representative ad hoc routing protocols. For the evaluated protocols, more extensive descriptions are provided in Section 3.

1.1.1. Proactive protocols

They are also known as state-based/table driven protocols. Protocols that fall in this category perform periodic route table exchanges and continuously attempt to maintain a complete topological view of the network at each node. Hence, routes are readily available when data need to be sent.

1.1.1.1 Link state

Fisheye State Routing [2]. The amount of link state information received depends on the distance from the source. Nodes exchange link state for distant nodes with lower frequency than for nodes within a specified scope. Correctness is maintained due to the fact that routing information becomes more accurate as it is forwarded towards the destination.

Optimized Link State Routing [3]. Each node selects a set of its neighbors to be its Multipoint Relay MPR nodes. Link state information regarding this node is periodically transmitted only by its MPRs. MPRs provide an efficient method for flooding control packets. MPRs calculate shortest paths for their selectors and are used to form routes to every destination.

1.1.1.2 *Distance vector*

Wireless Routing Protocol [4]. It is a table-based protocol aiming to maintain routing information among all nodes in the network. Update messages are periodically exchanged only between neighboring nodes and contain a list of update information such as the destination, the distance to the destination, and the second-to-last hop to the destination. Nodes do not exchange the whole distance vector table information , rather they exchange tuples that reflect link changes. If no changes occur, they only transmit Hello messages to maintain neighbor information. By maintaining predecessors of destinations it is able to recursively detect loops.

Destination Sequence Distance Vector [5]. This protocol augments the classical, distributed Bellman-Ford by tagging each distance entry $d_{ik}(j)$ by a sequence number that originated in the destination node i. Each node maintains this sequence number, incrementing it each time the node sends an update to the neighbors. The sequence number is disseminated in the network via update messages. The destination sequence number is used to determine the "freshness" of a route. Always the latest sequence number is used for updating routes. For equal sequence numbers, the one with the smallest distance metric is used. It has been shown that DSDV avoids long-lived loops and counting to infinity problems.

1.1.2. Reactive protocols

These protocols are also referred to as on-demand routing protocols, because nodes initiate route discovery via a request/ reply mechanism, only if the presence of the need to route a packet to a specific destination. As an optimization they, maintain a cache of soft-state route entries for future use.

Dynamic Source Routing, DSR [6]. It uses source routing, with each packet carrying in its network layer header the complete ordered list of the nodes it will pass. Routes are resolved through a flood based route discovery process during which the path is recorded in the control packets. The on-demand nature of the protocol eliminates the need for periodic updates and neighbor discovery beacons.

Ad Hoc On Demand Distance Vector, AODV [7]. It builds on DSDV's sequence number mechanism. Sequence numbers of control packets are used to ensure that paths are loop free and recent. Intermediate nodes update their forwarding tables during the reply phase of the route discovery. The back up routing mechanism of AODV-BR [8] provides resilience to frequent topology changes.

1.1.3. Zone-based Clustered Protocols

Zone Routing Protocol [9]. It is a zone or cluster-based routing protocol that combines the best of proactive and reactive routing protocols. Zone is an area within a specified range. Its operation is bimodal, utilizing proactive routing for intra-zone communications and reactive routing across zones. If the route to a node is not known, the request is broadcast to the zone perimeter and from that point further an on-demand protocol is used to establish the route. This protocol is intended for large scale networks where it makes sense to divide space into zones. Since our study focuses in relatively small scale, we are not including it in the evaluation.

1.1.4. Location Aware Protocols

Location Aided Routing [10]. This complementary protocol employs explicit location information to improve routing performance of on demand routing protocols. It enhances the flooding phase of the route discovery using location information.

1. 2. Table Driven And On-Demand Ad Hoc Protocols

Two different types of routing protocols: table driven link state protocol and source initiated on-demand routing protocol [1]. Table driven link state protocols where each node gathers information about the state of the links those are available and keep them in tables. The costs of the outgoing links are updated in these tables. Some of the transferred information could be outdated due to the propagation delays. These protocols require high bandwidth to keep links status information current. Some link-state protocols reduce the bandwidth by minimizing the transfer of state link information. They distribute the information only to the affected nodes.

On-demand protocols do not gather or distribute information unless there is a need to establish communication. There are no tables to maintain, and no data update is required. These protocols are efficient for Ad hoc networks since they minimize the overhead of routing.

2. PREVIOUS AND RELATED WORKS

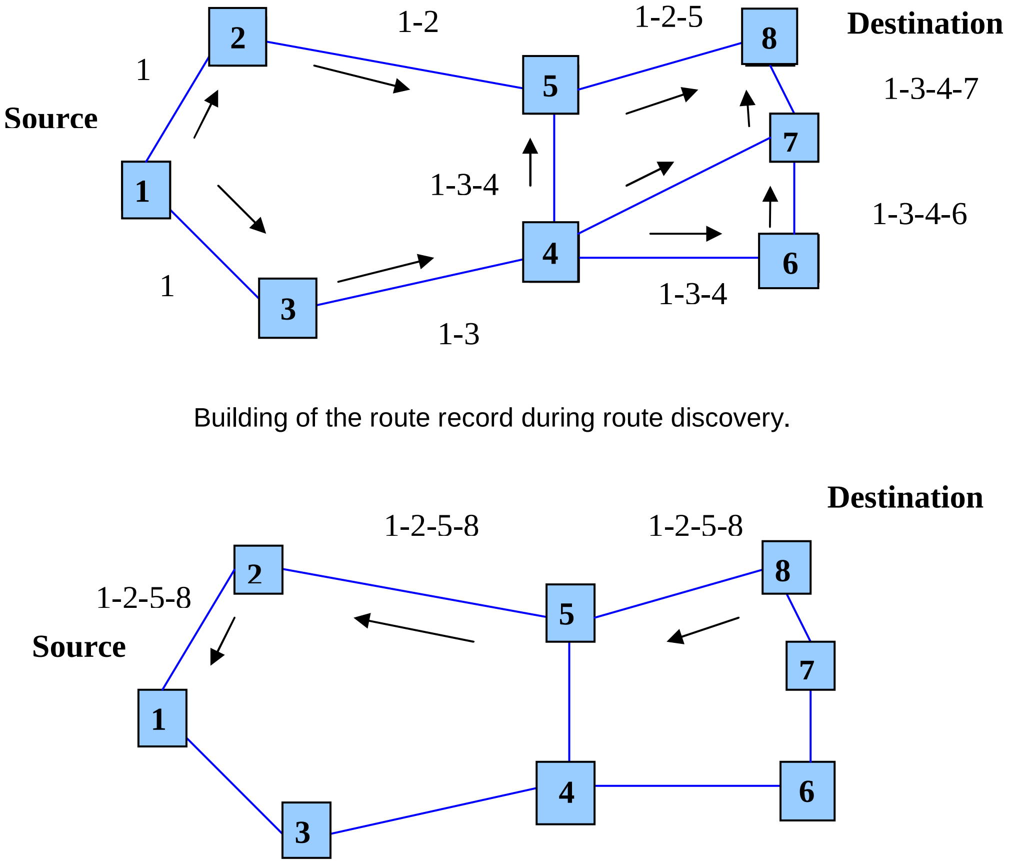
Due to nodes mobility, the topology of an ad hoc network may change rapidly and unpredictably over time. The design of network protocols for MANET is a complex issue, these networks need efficient distributed algorithms to determine network organization (connectivity), link scheduling and routing.

Most routing protocols for mobile ad hoc networks, such as: Ad Hoc On Demand Distance Vector Protocol (AODV), Dynamic Source Routing (DSR) are designed without explicity considering quality of service of the generated route. These routing protocols provide the capability for establishing minimum hop paths between nodes on a best effort basis regardless of QoS. In our work, we analyze the performance of these protocols and we present an efficient load-balancing scheme for support QoS over MANET that allows nodes to:

- Distribute and efficiently use network resources (buffer space),
- Reduce network congestion by change route,
- Increase overall performance (throughput).

2.1. Dynamic Source Routing (DSR)

DSR is a reactive ad-hoc protocol that employs source routing and aggressive route caching. Routes are resolved by flooding requests and source routed replies. The route discovery phase yields redundant routes to a destination because route destinations reply to all received requests. In the process, intermediate nodes in the reply path also resolve routes to this destination. If backward learning is enabled, assuming symmetric links, reversed routes are resolved upon reception of a request. Source routing enables DSR to detect loops and to acquire topological information by promiscuously listening to next-hop nodes transmissions. DSR assumes link layer failure feedback from the MAC layer. It uses this feedback, to initiate route failure to nodes in the upstream. The protocol consists of the two major phases of route discovery and route maintenance. When a node has a packet to send, it first looks up its cache to determine whether it already stores the routing information for the destination. If there is an unexpired corresponding entry then it utilizes it to source route. If there is no entry then it initiates route discovery by broadcasting a route request packet as in **Fig. 2**. This packet contains the destination address, the source's address and a unique identification number. Each node receiving the request, processes it to determine whether it is aware of a route to the destination. If it is not, it simply adds its own address to the route record of the packet and forwards the packet by re-broadcasting it with TTL 1. To prevent excessive flooding a node forwards the request only if it has not yet been seen by the mobile and if the host's address does not appear in the packet's route record .Each packet is uniquely identified by the sequence number/source id pair. Route replies are generated when the request reaches a node that has a fresh entry for the route to the destination or the destination itself as in **Fig. 2**. When the packet reaches the destination or an intermediate node, it contains the sequence of hops made. If the node is an intermediate node, it augments the received hop list with its own list and source routes the packet to the request originator using the reverse route. If symmetric links are not present, it will use an entry in its cache for the originator and in case there is no valid entry it will generate a route discovery request and piggy bag the route reply. Route maintenance is carried out using route error packets and acknowledgements. The first are generated at a node when the data link layer encounters a fatal transmission error. The error signifies that the downstream node is not accessible. In 802.11b, transmission errors are detected through the ACK mechanism. When a route error packet is received, the erroneous hop is removed from the node's route cache and all routes containing that node are truncated at that point, yielding routes to the destination that reported the error. As an optimization, a route to a destination is retrieved by scanning the cache for routes that go through the requested destination. In addition to route error messages, acknowledgments are used to provide verification on the correct operation of the route links. Passive acknowledgements are such a mechanism**,** where a host is able to determine whether the packet it just forwarded has been received and re-broadcasted by listening to the channel.



Building of the route record during route discovery.

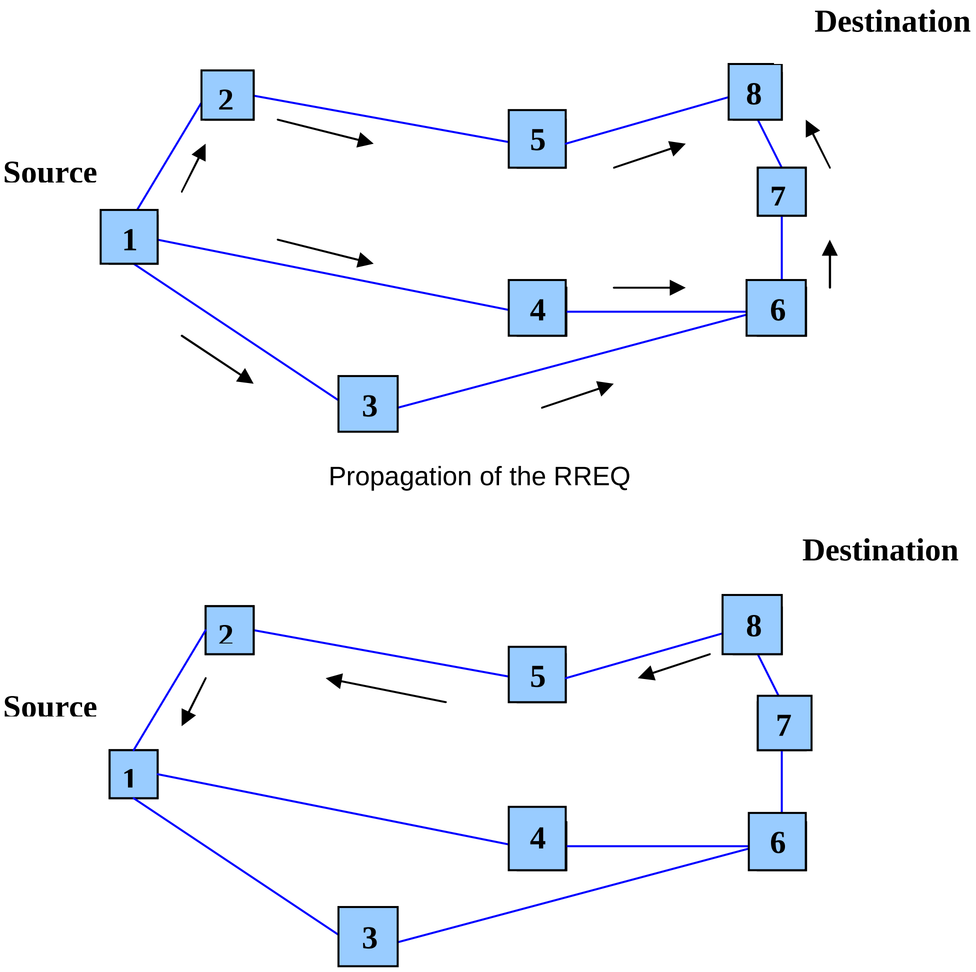
Propagation of the route reply with the route record.

Fig. 2: Creation of the route record in **DSR**.

2.2. Ad-hoc On-demand Distance Vector (AODV)

The Ad Hoc On-Demand Distance Vector (AODV) routing protocol described in [7] builds on the DSDV [5] algorithm. AODV is an improvement on DSDV because it typically minimizes the number of required broadcasts for creating routes on a demand basis, as opposed to maintaining a complete list of routes as in the DSDV algorithm. The authors of AODV classify it as a pure on-demand route acquisition system, since modes that are not on a selected path do not maintain routing information or participate in routing table exchanges. When a source node desires to send a message to some destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other node. It broadcasts a route request (RREQ) packet to its neighbors, which then forward this packet to their neighbors, and so on, until either the destination or an intermediate node with a .fresh enough. route to the destination is located. **Figure 3** illustrates the propagation of the broadcast RREQ across the network. AODV utilizes destination sequence numbers to ensure all routes are loop free and contain the most recent route information. Each node maintains its own sequence number, as well as broadcast ID. The broadcast ID is incremented for every RREQ the node initiates, and together with the node's IP address, uniquely identifies an RREQ. Along with its own sequence number and the broadcast ID the source node includes in the RREQ the most recent sequence number it has for the destination. Intermediate nodes can reply to the RREQ only if they have a route to the destination whose corresponding destination sequence number is greater than or equal to that contained in the RREQ. As an optimization, RREQ flood is controlled using expanding ring search. During the process of forwarding the RREQ, intermediate nodes record in their route tables the address of the neighbor from which the first copy of the broadcast packets received, thereby establishing a reverse path. If additional copies of the same RREQ are later received, these packets are discarded. Once the RREQ reaches the destination or an intermediate route with a fresh enough route, the destination/ intermediate node responds by unicasting a route reply (RREP) packet back to the neighbor from which it first received the RREQ.

As the RREP is routed back along the reverse path, nodes along this path set up forward route entries in their route tables which point to the node from which the RREP came. These forward route entries indicate the active forward route. Associated with each route entry is a route timer which will cause the deletion of the entry if it is not used within the specified lifetime. Because the RREP is forwarded along the path established by the RREQ, AODV only supports the use of symmetric links. Routes are maintained as follows. If a source node moves, it is able to reinitiate the route discovery protocol to find a new route to the destination. If a node along the route moves, its upstream neighbor notices the move and propagates a link failure notification message to each of its active upstream neighbors to inform them of the erasure of the part of the route. These nodes in turn propagate the link failure notification to their upstream neighbors, and so on until the source node is reached. The source node may then choose to reinitiate route discovery for that destination if a route is still desired. An additional aspect of the protocol is the use of hello messages, periodic local broadcasts by a node to inform each mobile node of other nodes in its neighborhood. Hello messages can be used to maintain the local connectivity of a node. However, the use of hello messages is not required. Nodes listen for retransmission of data packets to ensure that the next hope is within reach. If such a retransmission is not heard, the node may use any one of a number of techniques, including the reception of hello messages, to determine whether the next hop is within communication range. The hello messages may list the other nodes from which a mobile has heard, thereby yielding greater knowledge of Network connectivity.



Propagation of the RREQ

Path of the RREP to the source

Fig. 3: AODV route discovery.

3. A CRITIQUE OF DSR AND AODV

The two on-demand protocols share certain characteristics. In particular, they both discover routes only when data packets lack a route to a destination. Route discovery in either protocol is based on query and reply cycles, and route information is stored in all intermediate nodes along the route in the form of route table entries (AODV) or in route caches (DSR). However, there are several important differences in the dynamics of these two protocols, which may give rise to significant performance differentials.

First, by virtue of source routing, DSR has access to a significantly greater amount of routing information than AODV. For example, in DSR, using a single request-reply cycle, the source can learn routes to each intermediate node on the route in addition to the intended destination. Each intermediate node can also learn routes to every other node on the route. Promiscuous listening of data packet transmissions can also give DSR access to a significant amount of routing information. In particular, it can learn routes to every node on the source route of that data packet. In the absence of source routing and promiscuous listening, AODV can gather only a very limited amount of routing information. In particular, route learning is limited only to the source of any routing packets being forwarded. This usually causes AODV to rely on a route discovery flood more often, which may carry significant network overhead.

Second, to make use of route caching aggressively, DSR replies to all requests reaching a destination from a single request cycle. Thus, the source learns many alternate routes to the destination, which will be useful in the case that the primary (shortest) route fails. Having access to many alternate routes saves route discovery floods, which is often a performance bottleneck. However, there may be a possibility of a route reply flood. In AODV, on the other hand, the destination replies only once to the request arriving first and ignores the rest. The routing table maintains at most one entry per destination.

Third, the current specification of DSR does not contain any explicit mechanism to expire stale routes in the cache, or prefer “fresher” routes when faced with multiple choices. As noted in [11], stale routes, if used, may start polluting other caches. Some stale entries are indeed deleted by route error packets. But because of promiscuous listening and node mobility, it is possible that more caches are polluted by stale entries than are removed by error packets. In contrast, AODV has a much more conservative approach than DSR. When faced with two choices for routes, the fresher route (based on destination sequence numbers) is always chosen. Also, if a routing table entry is not used recently, the entry is expired. The latter technique is not problem-free, however. It is possible to expire valid routes this way if unused beyond an expiry time. Determination of a suitable expiry time is difficult, because sending rates for sources, as well as node mobility, may differ widely and can change dynamically. In a recent paper [12], the effects of various design choices in caching strategies for on-demand routing protocols are analyzed.

Fourth, the route deletion activity using RERR is also conservative in AODV. By way of a predecessor list, the error packets reach all nodes using a failed link on its route to any destination. In DSR, however, a route error simply backtracks the data packet that meets a failed link. Nodes that are not on the upstream route of this data packet but use the failed link are not notified promptly.

4. MODIFICATIONS AND OPTIMIZATIONS

In HDSR we classify the participating nodes of the network as Mobile Node (MN) and Forwarding Node(FN). We assign different functionalities to those nodes depending on what type of node they are. MNs initiates route discovery. FNs help them to find source route to the destination MN. The destination MN replies back through the FNs to source MN. Once source MN discovers the routes, it starts sending packets to the destination. FNs assist the MN to forward packets to destination MN. Route discovery and route maintenance in this technique are different from those in DSR. When a source MN originates packet to a destination MN. If the source cannot find a source route in its route cache, it initiates a route discovery by transmitting a "route request packet" as a local broadcast packet. Only FNs, which are within the range of the source MN receives the broadcast packet. Other MNs, which are also within the range of source MN and which are not the destination of this packet, discard the broadcast message and do not broadcast further. Only the FNs re-broadcast the request to other FNs unless the destination MN receives this route request packet. The destination MN then replies back to the source MN through the FNs. After receiving the route reply, the source MN record the source route in its cache and starts sending packets to the destination MN using the source route it has just discovered.

Route maintenance is performed by FNs only. When a FN detects that the next link from itself to the next MN or FN is broken, it updates that its own route caches by marking all the paths which use the broken link as invalid and sends route error message to the source MN and all other FN which uses the broken link for packet transmission. We will explain now how it reduces overhead packet during the route discovery processes and prevent route request and route reply flooding.

Figure 4 shows how a route is discovered. In this scenario nodes 1,2,3,5 and 6 are MNs and nodes 4 and 7 are FNs. Route discovery is initiated by MN-1 to find a source route to destination MN-8. MN-1 transmits the route request packet as a local broadcast message. MN-2, MN-3 and FN-4 are within the range of MN-1. MN-2 and MNB-3 are restricted not to re-broadcast the route request further. They are not forwarding nodes and they are not the destination as well. Only FN-4 will rebroadcast the request packet after adding itself in the request packet. FN-7 will only accept the route request packet only because it is the only FN within the range of FN-4. FN-7 rebroadcast the request packet and the route request packet finally reaches the destinationMN-8. MN-8 replies back to source node. Upon receiving the reply packet, source MN-1 record its route cache and starts sending packet through the source route it has just learned from the reply packet. In this case only three broadcast messages are generated. Redundant route request broadcasting by MNs except the source MN has been eliminated which saves bandwidth by reducing packet collision. **Figure 5** illustrate how route reply flooding is prevented. In this case there is only one FN and all other nodes are MNs. Route discovery was initiated by MN-1 to find a source route

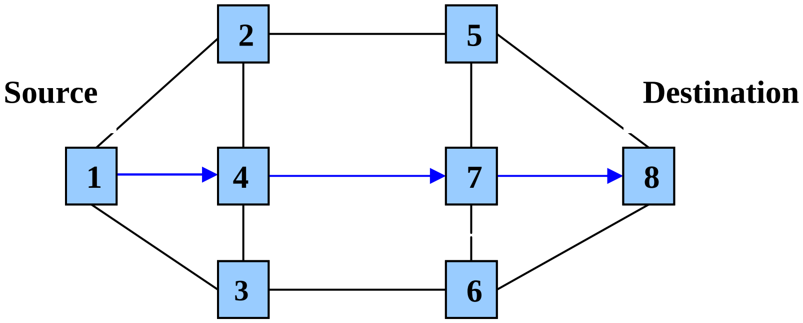


Fig. 4: Limiting Route Reply storming.

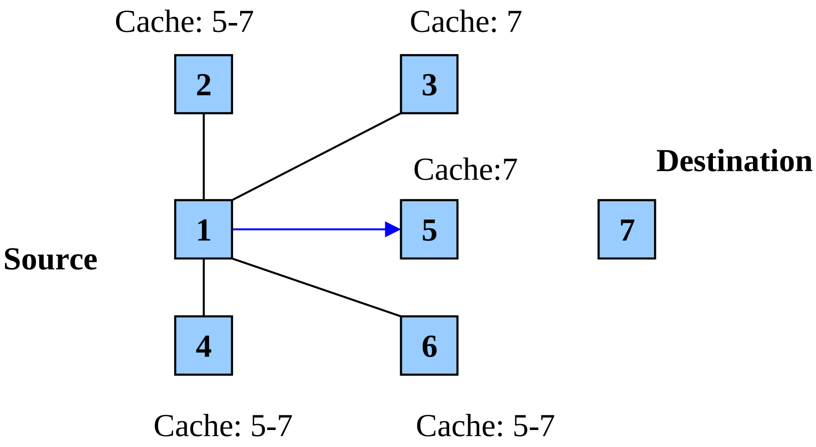


Fig. 5: Limiting Route Request.

to the destination MN-7. MNs 2,4,5,6 and FN-3 are within the range of MN-1. Assume each MN and FN has a source route in its cache. In our case, only FN-3 will reply back to MN-1 in contrary to replying procedure used in DSR where all the MNs reply back to MN-1. All other MNs which received the route request message discard it. MN-1 starts sending packet to destination MN using the route 1-3-7. Thus route reply flooding is limited in our case when each node replies from its route cache.

5. SIMULATION MODEL AND RESULTS

Network Simulations used to implement and test the performance of these protocols. The key parameters are summarized in **Table 1** below. **Figures 6, 7, 8** show performances of simulations of 80 MNs scenario versus the pause time of mobile nodes. The size of the rectangular area that mobile nodes are located is 1000x1000 meters. There are 20 CBR sources with data packet rate of 2 packets per seconds, 12 FNs in additions to MNs and locations of the FNs are chosen randomly as well. (**Figure 6**) shows the routing overhead of the protocols. The routing overhead in this technique (HDSR) is consistently lower than DSR in all scenarios, and for this scenario it is approximately 50 times lower. We observed that overhead improvement in this technique is higher when the number of nodes in the networks grows. The difference between this technique and DSR overhead increases when the mobility is higher (i.e., shorter pause times). Due to the higher number of routing overhead packets, the network with DSR routing protocol has lower bandwidth for data packets, which we think adversely affects performance metrics in DSR compared with this technique. For example, throughput of the network is improved 3 times in high mobility and 20-30 percent in low mobility cases compared with that of DSR (**Figure 7**). In different scenarios, the throughput is always better with this technique. The average end-to-end delay is also improved.(**Figure 8**) shows average end-to-end delay of scenario with 80 mobile nodes.

Table 1: Simulation Parameters.

Parameter	Value
Transmission Range	250 Meters
Medium Access Control (MAC)	IEEE802.11
Raw Capacity	2 m/s
Traffic Sources(CBR)	512 b/s
Mobility Model	Waypoint model
Speed	0-20 m/s

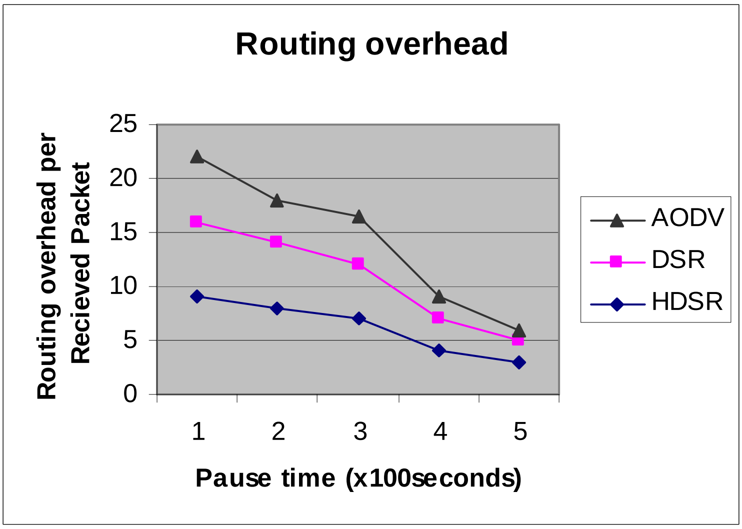


Fig. 6: 80 MN Scenario.

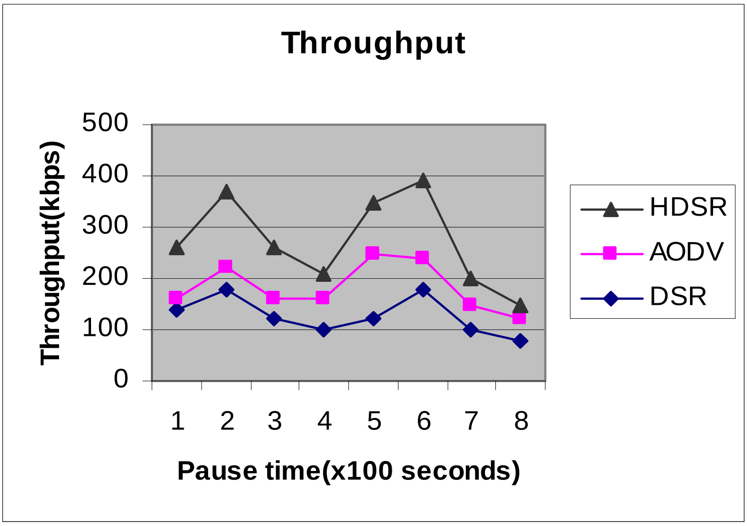


Fig. 7: 80 MN Scenario.

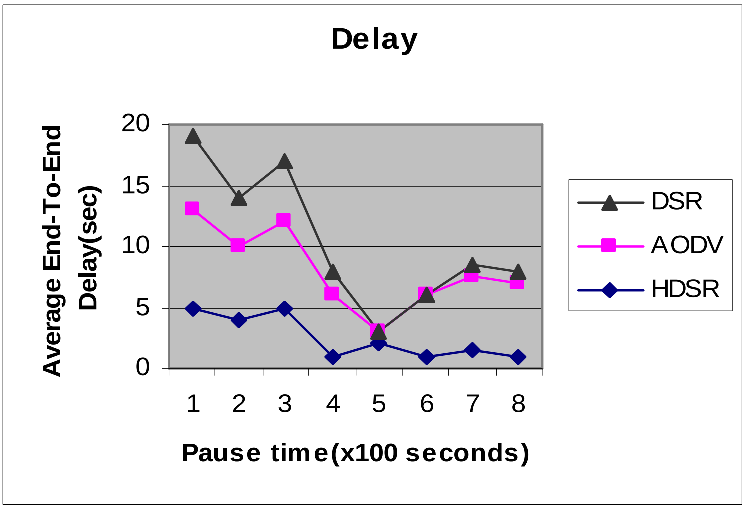


Fig. 8: 80 MN Scenario.

In that case, the delay is 3 times higher than that for very high mobility (i.e. pause time less than 50 seconds) and few tens of times in low mobility cases. Delivery ratios was better than DSR too. (**Figure 6**) shows how this technique saves overhead which results better throughput (**Figure 7**). Number of FNs in the network naturally affects the performance of this technique. We observed that increasing the number of FNs in the network improves the throughput up to a certain point. That is why we think that distribution of FNs in the network is important for optimization of the performance figures, and we will consider this point in the future work. We consider an example scenario corresponds to a network of 100 nodes with zero pause time (constant mobility). Traffic in this example involves 40 CBR sources each generating packets at the rate of 2/s, each of size 512 bytes. For this example, the application-oriented metrics point out that DSR has a nearly 32 percent lower delivery fraction than AODV and 5 time's higher delay. But for HDSR, DSR has a nearly 45 percent lower delivery fraction than HDSR and few 10 times higher delay.

Table 2: Results.

Performance metrics	**DSR**	**AODV**	**HDSR**
Packet delivery fraction (%)	56.88	83.66	90.48
Average delay (s)	1.36	0.26	0.14

6. CONCLUSIONS

We have compared the performance of DSR and AODV, two prominent on-demand routing protocols for ad hoc networks. DSR and AODV both use on-demand route discovery, but with different routing mechanics. In particular, DSR uses source routing and route caches, and does not depend on any periodic or timer-based activities. DSR exploits caching aggressively and maintains multiple routes per destination. AODV, on the other hand, uses routing tables, one route per destination, and destination sequence numbers, a mechanism to prevent loops and to determine freshness of routes. We observed that These routing protocols provide the capability for establishing minimum hop paths between nodes on a best effort basis regardless of QoS. In this paper, we have defined an efficient technique for supporting QoS in Mobile Ad Hoc Networks named Hierarchical Dynamic Source Routing protocol (HDSR). This technique is able to improve network performance figures, namely throughput, delay and packet delivery ratio significantly. Our future work is to define a new parameters to provide load balancing, support fault tolerance, and select optimal routes.

7. REFERENCES

[1] Chrles E. Perkins, The Ad Hoc Network, Boston, 2001.

[2] G. Pei, M. Gerla, and T.-W. Chen, .Fisheye state routing in mobile ad hoc networks,. Proceedings of the 2000 ICDCS Workshops, Taipei, Taiwan, Apr. 2000, pp. D71-D78.

[3] P. Jacquet, P. Muhlethaler, and A. Qayyum, .Optimized link state routing protocol,. IETF MANET, Internet Draft, Nov. 1998.

[4] S. Murthy and J. J. Garcia-Luna-Aceves, .An ef_cient routing protocol for wireless networks,. ACM Mobile Networks and Applications Journal, Special issue on Routing in Mobile Communication Networks, 1996.

[5] C. E. Perkins and P. Bhagwat, .Highly dynamic destination sequenced Distance vector routing (dsdv) for mobile computers, ACM SIGCOMM: Computer Communications Review, vol.24, no.4, pp.234-244, October 1994.

[6] D. B. Johnson and D. A. Maltz, the dynamic source routing protocol for mobile ad hoc networks,. Mobile Computing, edited by Tomas Imielinski and Hank Korth, Kluwer Academic Publishers, ISBN: 0792396979, 1996, Chapter 5, pages 153-181.

[7] C. E. Perkins and E. M. Royer, .Ad-hoc on-demand distance vector routing,. second IEEE Workshop on Mobile Computing Systems and Applications, pp.90-100, February 1999.

[8] S. J. Lee and M. Gerla, .aodv-br: Backup routing in aodv,. in Infocom 2003.

[9] Z. Haas and M. Pearlman, .The zone routing protocol (zrp) for ad hoc networks,. IETF Internet Draft, Version 4, July, 2002.

[10] Y. Ko and N. H. Vaidya, .Location aided routing (lar) mobile ad hoc networks,. MOBICOM 1998.

[11] D. Maltz et al., “The Effects of On-demand Behavior in Routing Protocols for Multihop Wireless Ad Hoc Networks,” IEEE JSAC, vol. 17, no. 8, Aug. 1999.

[12] Y. C. Hu and D. Johnson, “Caching Strategies in On-demand Routing Protocols for Wireless Ad Hoc Networks,” Proc. IEEE/ACM MOBICOM ’00, Aug. 2000, pp. 231–42.

تقييم أداء البروتوكولات المستخدمة في شبكات ال ad-hoc اللاسلكية

تعتبر شبكات ال **ad-hoc** اللاسلكية شبكات حديثة نوعا ما وأصبح لها وجود في مجال البحث العلمي. تتميز هذه الشبكات بعدم وجود شكل أو تنظيم ثابت لها، حيث أنها شبكات ذاتية التنظيم. وقد ظهر العديد من البروتوكولات المستخدمة في هذه الشبكات والتي تختلف في إنجازاتها ومدى تعقدها. أغلب هذه البروتوكولات تم تصميمها لإيجاد أقصر مسار لنقل البيانات دون مراعاة مستوى جودة الخدمة. يقوم هذا البحث بتحليل أداء هذه البروتوكولات عن طريق دراسة مجموعة من المعايير كما يقوم بعرض تكنيك فعال يدعم جودة الخدمة على هذه الشبكات.