Extension of Dynamic Source Routing Protocol in Mobile Ad hoc Network

Osman Ghazali [1], Suhaidi Hassan[2], Naseer Ali [3], Nur Ziadah Harun[4], Saichai a/p Eh Song[5], Norhidayah Abdullah[6]

Graduate Department of Computer Science, College of Arts and Sciences,
University Utara Malaysia
06010 UUM Sintok, Malaysia
Email: osman@uum.edu.my[1], suhaidi@uum.edu.my[2], naseer.iraq@yahoo.com[3], s71497@student.uum.edy.my[4], s803132@student.uum.edu.my[5], s803125@student.uum.edu.my[6]

ABSTRACT

An ad hoc mobile network is a collection of mobile nodes that are dynamically and arbitrarily located in such a manner that the interconnections between nodes are capable of changing on a continual basis. In order to facilitate communication within the network, a dynamic source routing protocol can be used to discover routes between nodes. The primary goal of such an ad hoc routing protocol is to achieve correct and efficient route establishment between a pair of nodes so that message can be delivered in a timely manner. Each node in mobile ad hoc network (MANET) can function as both a host and a router. The network topology is dynamic because the connectivity among the nodes may vary with time due to node mobility, node departures, and new node arrivals. Hence, there is a need for dynamic routing protocols to allow the nodes to communicate. In this paper, we survey and compare DSR's extensions.

Keywords:
ad hoc network, MANETs, Routing Protocol, DSR

1. Introduction

Mobile ad-hoc network (MANET) is a dynamic and autonomous network composed of wireless mobile hosts or nodes. It is an autonomous system that composed of mobile nodes. The ad hoc topology may change with time as the nodes join or move from the network. The system may operate in isolation or may have gateways that connected to a fixed network.

MANETs have several salient characteristics:

- **Dynamic topologies**: the network topology may change randomly and rapidly at unpredictable times, and may consist of both bidirectional and unidirectional links.
- **Bandwidth-constrained links**: the wireless links will continue to have significantly lower capacity than their hardwired counterparts.
- **Energy-constrained operation**: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes, the most important system design criteria for optimization may be energy conservation.
- **Limited physical security**: mobile wireless networks are generally more prone to physical security threats than fixed networks. The increased possibility of eavesdropping, spoofing, and denial-of-service attacks should be carefully considered mobile wireless networks.

The characteristics of MANET create a set of underlying assumptions and performance concerns for protocol design, which extends beyond those guiding the design of routing within the higher-speed, semi-static topology of the fixed Internet. DSR is a potential routing protocol to be used in MANET, where it is designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.

This paper attempts to survey the extensions of DSR for MANET. It is organized as follows: In section 2, basic of DSR is introduced. Then extensions of DSR are described in section 3. Section 4 presents discussion about advantages of DSR's extensions, conclusion and future work for DSR extension.

2. Dynamic Source Routing

DSR is a simple and efficient routing protocol designed specifically for use in MANET. It allows the network to be completely self-organizing and self-configuring without the need for any existing network infrastructure or administration. The protocol composed of two main mechanisms, namely Route Discovery and Route Maintenance. The mechanisms work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network Follows are the characteristics of DSR: easily guaranteed loop-free routing, operation in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change.

In DSR, Route Discovery and Route Maintenance each operate entirely "on demand". DSR requires no periodic packets of any kind at any layer within the network. For example, DSR does not use any periodic routing advertisement, link status sensing, ad neighbor detection

packets. Also, it does not rely on these functions from any underlying protocols in the network. As this is entirely on demand, lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero.

The operation of both Route Discovery and Route Maintenance in DSR are designed to allow unidirectional links and asymmetric routes to be supported. In route discovery process, when a source node attempt to send packets to a destination, it first checks whether it has a route to this destination in the route cache. If not, the source node will initiate a route request (RREQ) packet for broadcast. Nodes receiving this RREQ will first see whether the destination is itself. If yes, it will reply with a route reply (RREP) packet unicast to the source node with the reverse path the RREQ traversed. Otherwise this node is an intermediate node. Intermediate nodes who receive this packet should first check the freshness of this RREQ. If the intermediate nodes have received this RREQ recently it will ignore the packet, else the intermediate node will rebroadcast this RREQ. Another alternative is that the intermediate node replies the RREQ when it knows a route to the destination. Figure 1 shows the formation of route record as the RREQ broadcasted through the network, while Figure 2 shows the unicast of RREP with route record from destination to the source. Source node should be notified using route error (RERR) packets when there is a break on any link on the route that is in use. Source node receiving the RERR will delete all the routes which contain the reported link. A new RREQ will be generated when the route is still needed.

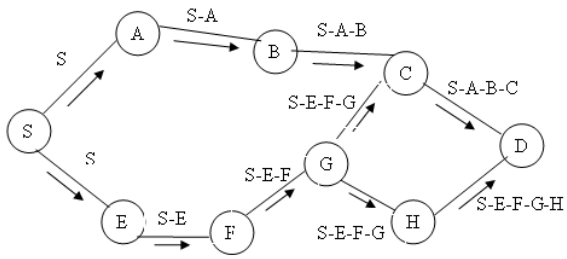


Figure 1: Building of Route Record during Route Discovery

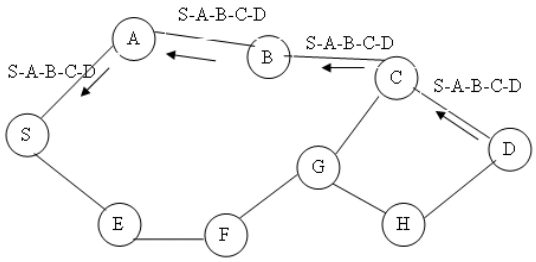


Figure 2: Propagation of RREP with Route Record

3. Extension of DSR

This section discusses about various extensions of DSR. Previously, many researchers had designed extensions and performed experiments to improve the weakness of traditional DSR. This paper provides a review and comparison on the extensions of DSR that include Multipath DSR (MPDSR),

3.1 Multipath DSR

The objectives of Multipath DSR (MPDSR) are to provide a reliable route for packet transmission with minimum overhead and to improve Quality of Service (QoS) support with respect to end-to-end reliability. The technique used in this protocol is forwards outgoing packets along multiple paths that are subject to a particular end-to-end reliability requirement (Leung, Liu, Poon, Chan & Li, 2001). There have several types of Multipath DSR, i.e. Multipath Source Routing (MSR), Robust Multipath Source Routing (RMPSR), Enhanced DSR with Secure Multipath Route Discovery (SDSR) and Cluster-Based Multipath DSR (CMDSR).

MSR is an extension of DSR that uses the same route discovery process as in DSR. The improvement of this protocol over traditional DSR is better distribution of traffic among multiple routes in the network. In MSR, all possible source to destination path will be selected and store it in the table. To deal with multipath routing, MSR extends DSR's Route Discovery and Route Maintenance Mechanism by incorporating the multipath mechanism into DSR and employing a probing base load balancing mechanism (Wang, Zhang, Shu & Dong, 2000).

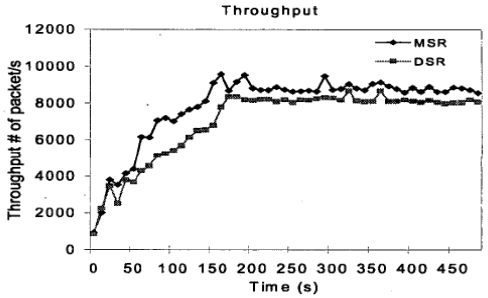


Figure 3: Comparison of Throughput (Wang, Zhang, Shu & Dong, 2000)

MSR achieve better performance than DSR, where it is clearly can be seen in Figure 3 that during the simulation MSR achieve higher throughput than DSR almost at every time point. This is due to the fact that the multi-path routing used the unallocated network resource more effectively than DSR.

Wei and Zakhor (2004), proposed RMPSR that extends DSR to support multipath video communication over wireless ad ho networks. The main goal of RMPSR is to minimize video packet loss caused by network topology changes. Multipath routing is important for video communication application

over wireless ad hoc network, especially for near live video application. Since connectivity along multiple paths is less likely to be broken than connectivity along the single path, these resulting a more smooth video delivery. Techniques use in RMPSR is a per-packet allocation scheme to distribute video packet over two primary routes of two route sets. When one transmitting primary route is broken, the intermediate node that corresponds to the broken link will send a Route Error (RERR) packet to the source node. Upon receiving the RERR packet, the source node removes the broken primary route from its route cache, and switches the transmission to another primary route. Three schemes are introduced to support video application. The first scheme is when the transmitting route is broken, alternative routes in the same route set will be used to forward packets that are in the mid way. This will save the packets from being dropped. The advantage of this scheme is increase in delivery ratio of video packet without retransmission. The second scheme is RMPSR triggers new route request process before the connectivity is entirely loss. This scheme is able to reduce the number of temporary network outages during the transmission. For the third scheme, RMPSR increase the probability of discovery multiple disjoint routes at by including more information in the communication. This increases control overhead. To maintain high quality of video application when the number of data traffic in the network increase, RMPSR give higher priority to video traffic.

Rawat and Vyavahare (2006) proposed SDSR. The purpose of their work is to provide security in DSR routing by integrating Secure Routing Protocol features into DSR functionalities. It exploits multiple routes for data transmission phases based on Secured Message Transmission (SMT) technique. SMT exploits multiple routes in transmitting data from the source to the destination. The data from the source will be dispersed into several packets, e.g. P packets. The packets are routed through multiple routes simultaneously. At the destination, reconstruction of the original packet can be ensured by receipt of Q out of P packets. Figure 4 shows how ACK and dispersed packets flow from source to destination. If data packet is dispersed into four parts (P = 4), then, three out of four packets (Q=3) are sufficient to reconstruct the original message.

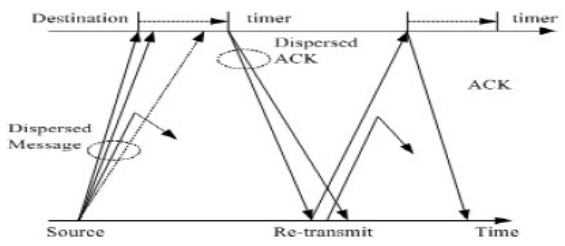


Figure 4: Sample Example of SMT Protocol

The source dispersed SMT data packets into multiple packets and sent them through multiple routes simultaneously. Two packets out of four data packets are received at destination and two are lost. Destination extract information from the first received packet, set reception timer and wait.

The receiver generates acknowledgement for the two successfully received packets on expiry of the timer. On receipt of the ACK, source rejects the two failing routes and retransmits the two packets. One of the retransmitted packets is again compromised. Message at the destination will be reconstructed when have three out of four packets. Before timer expiry, the receiver acknowledges successful reception.

Zhong et al. (2005) proposed CMDSR that enhance the scalability of the DSR. The protocol is adaptive to the network dynamics, where it uses the hierarchy to perform route discovery and traffic distribution to multiple paths.

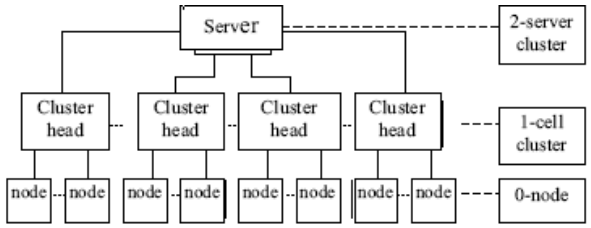


Figure 5: Cluster Architecture

Figure 5 shows CMDSR consist of 3-level hierarchical scheme i.e. 0-node, 1-cell cluster and 2-server cluster. The first level of cluster is the 1-cell cluster. Server acts as leader which is gathered by 2-server cluster. To prevent the network flooding due to the DSR Route Discovery, server transfers the Route Discovery procedure to the 2-server level. Thus, Route Discovery does not require flooding mechanism and overhead is minimized.

3.2 Hierarchical DSR (HDSR)

Tarique et al. (2005) proposed HDSR that is derived from DSR. The forwarding nodes in HDSR are selected on demand and distributely. HDSR improves the performance of DSR by limit the number of node that participates in route discovery phase. There are 2 states of mobiles nodes, i.e. Mobile Node (MN) and Forwarding Node (FN). The protocol ensures that FNs are selected so that every source node can reach the destination and reduces the number of nodes required to respond and request message.

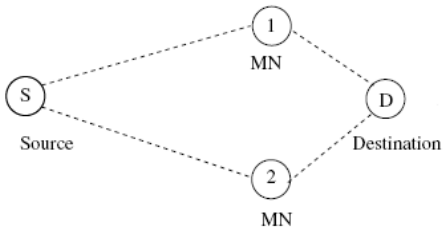


Figure 6: Transition from MN to FN

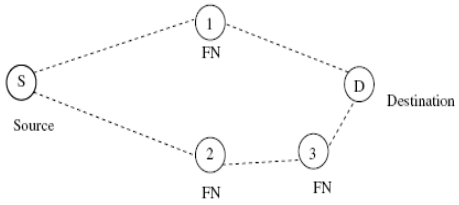
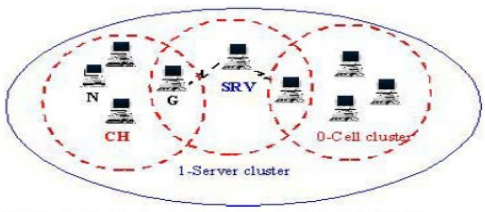


Figure 7: Transition from FN to MN

Figure 6 and 7 illustrate the operation of HDSR protocol. In MN state, a node act as either source or destination. While in FN state, a node forwards packets for other node. Only FNs participate in the route discovery. FN selection depends on route discovery message, so it does not require additional control message. HDSR will reduce the routing overhead significantly because the proposed algorithm works in the route discovery phase that reduces flooding. HDSR does not need to maintain any statistical information about the neighbors and location of the node.

3.3 Adaptive Cluster Source Routing (ACSR)

Jaddi and Paillassa (2005), proposed ACSR to increase the scalability of DSR with regards to network size and network mobility in an adaptive way. This protocol manipulates the adaptability of DSR and the routing mechanism of CSR to produce less overhead and perform efficient routing. Figure 10 illustrates the CSR model. CSR contains 2-level hierarchical architecture. The lower level is 0-cell cluster. Gateway nodes were used to established communication between 0-cell clusters. Each node within the cell is one hop away from the cluster head. The 1–server cluster, i.e. the upper level, is formed by several 0-cell clusters. Cluster leader is named as server.



N: Node, G: Gateway, CH: Cluster Head, SRV: Server

Figure 8: ACSR Model

3.4 Abbreviated DSR (ADSR)

In DSR a packet carries addresses of nodes for a path. This increases the size of a packet because the size will increase when the number of nodes in a path increases. One way to reduce the header size are by reduced the address's size and the route's size. ADSR is proposed to reduce protocol overhead by using abbreviated address. However, the abbreviation procedures can lead to two difference node having the same address which will cause collision. ADSR eliminates this collision problem by using hashing algorithm (P´erez, Olivera & Merino, 2005).

3.5 Pre-emptive DSR (PDSR)

In traditional DSR, every time when established path break a new route had to be discovered for communication between source and destination. To avoid this problem, PDSR is proposed based on a backup route i.e. second best route (Maity et al., 2008) as shown in Figure 9.

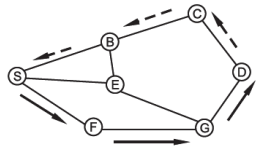


Figure 9: Primary and Backup Routes

Primary Route → <S,F,G,D>
Backup Route →<S,B,C,D>

<S,F,G,D> is the primary route for the destination D while the route <S,B,C,D> will be the backup route. Destination node (D) sends RREP packets to the source node (S) through the primary route and the backup route. When the source node receives the RREP packets, it starts communicating through the primary route and keeps the backup route in the Route Cache. During transmission of packets, e.g. if node F detects the signal strength falls below the threshold, it will send warning message to node S. The node S will immediately switches the transmission of packets through the backup route and sends the primary route for repairing. As transmission goes on through the backup route, node S tries to find a route by searching a succeeding node of the failed node F by the DSR. As a route from S to G is discovered, say as <S, E, G>, the route <S, E, G, D> is treated as the repaired route and is stored in the Route Cache of the source node S as the backup route.

3.6 Distance DSR (DDSR)

DDSR introduced new route maintenance strategy that utilizes location information called the DISTANCE (DIstance baSed rouTe maintenANCE) algorithm. In traditional DSR, if

alternative routes are not available during route maintenance, source node need to reinitiates route discovery to find new routes. So, the DISTANCE algorithm works by adding another node (called bridge node) into the source list to prevent the link from failure. There are two main components in modified route maintenance state that are used in DDSR i.e. route failure detection and route failure prevention. Route failure detection may detect failure link using three methods. First method is using hello message to determine link existence. Second method is using Medium Access Control (MAC) layer feedback. This method gives routing protocol quick response to link failure. The last method is using passive acknowledgement. This method detects link failure by overhears whether the next hop forward the packet further along the path. The link is considered fail if it does not listen the packet being forward by the next hop.

The second component, that is Route failure prevention, operates when a link is detected in unsafe conditions, i.e. the cost of the link is more than the threshold. If the node is in unsafe condition then the active node will send a one-hop packet to its neighbors for finding a bridge node. Bridge node is used for bridging current link to the next-hop node (Sjaugi, Othman & A.Rasid, 2008).

3.7 Active Packets improve DSR (Active DSR)

With the increases in network size and node mobility, cached routes quickly become inefficient because it cannot handle floods of route requests. Active DSR presents expandable active network approach to this route cache problem (He, Y., & Raghavendra, 2002). In Active DSR, an active packet roams around the network to gather network topology information. By checking the content of this active packet, network nodes are able to update their route caches. Thus cache miss rates and the route discovery flooding are reduced. The basic operation of Active DSR is to drive the active packet to visit each node twice. During first visit, the connection matrix of the active packet keep being added to topology information until the first visit is completed. For the second visit of the active packet, there is an active helper module that operates on a predefined active packet. The active helper validates and updates the route cache of a node according to the connection matrix in the active packet. In the validation phase, each routing entry is checked against the connection matrix and disagree routing entry are removed so that the flooding coming from route failures will be reduced.

3.8 Minimum Energy DSR (MEDSR)

Tarique and Islam (2007) proposed MEDSR approach to avoid additional existing control message of traditional DSR protocol. MEDSR works in two phases, i.e. route discovery and link by link power adjustment. In the route discovery mechanism, a source node uses two power levels i.e. low power level and high power level to discover a destination node.

At first, a source node initiates the route discovery to find a route to its destination by broadcasting a request packet at low power level. If the source node discovers a path using that low power level, it sets up a connection using that low power level. At a certain times, if a source node cannot discover the route to its destination using that low power level then it assumes the destination is not reachable at that low power level. Therefore, it will use high power level to initiate route discovery again. Once a route is discovered, the links by link transmit power of those power levels is adjusted to save more energy.

3.9 Extended DSR (EDSR)

EDSR is a new approach based on friendship between nodes which makes the nodes to co-operate in an ad-hoc environment (Raghavan, Labbai, Bhalaji & Kesavan, 2006). The scheme in EDSR can be categorized into 3 steps:

- Identification of relationship between neighbors in an ad hoc network i.e. stranger, acquaintance and friend.
- Routing mechanism
- Friends who turn malicious

In the first step, this protocol identifies the relationship of node *i* to it neighbor node *j*. In the second step, the routing mechanism starts when any node wants to send message to destination node that it sends a RREQ to all neighboring node. The RREP obtained from its neighbor is sorted by trust ratings. The level of trusted path is friend, acquaintance, followed by stranger. Trust relationship is based on experienced, observed, or reported routing and forwarding behavior of other nodes. The source selects the most trusted path to establish communication with the destination. Lastly, malicious node is detected in each node before starting the data transfer. It may involve the trust evaluator for a specific interval of time to reestablish the trust levels.

4. CONCLUSION

In this paper, we present the Dynamic Source Routing extension. They can be used to adapt DSR to various conditions of mobility and density. We provided overview of the DSR and how extension of DSR could fit into the specific conditions of ad-hoc network. Summary of the extensions is provided in Table 1.

There are several future work can be suggested for the current DSR. The future work for PDSR protocol maybe carried out over the calculation of the optimum value of the threshold

(Maity et al., 2008). In MEDSR, congestion aware must be modifying. The performance of MEDSR protocol needs to be compared with other energy aware routing protocols in order to see its advantages. Another future work is for EDSR. Performance analysis can be done on the extended protocol by introducing possible attacks.

MP-DSR Increase application performance by giving the application freedom to use multiple paths within the same path services.
MSR Achieve higher throughput than DSR almost at every time point and reduces end-to end delay and queue size while adding little overhead.
RMPSR Decreases the network congestions quite well and minimizes video packet loss caused by network topology changes
SDSR Provide security in DSR routing by integrating Secure Routing Protocol features into DSR functionalities.
CMDSR Produces less overhead and efficiency routing to achieve performance over high-density and low-mobility network.
HDSR Improves throughput performance of network by reducing the control overhead, and increases energy efficiency which is always desirable in mobile network environment Delay may increase if all the intermediate nodes in a single path between source and destination wait for random back-off delay before forwarding the request packet.
ADSR Reduce header size, allowing not unique identifier
PDSR Number of parallel route, the most stable for communication . The drawback of PDSR is the environment is highly dynamic by nature there is a high probability that the backup route will fail by the time primary route break.
DDSR Increase the average number of packet delivery ratio because DDSR algorithm provides proactive method to prevent route failure. So, it could reduce the number of route re-establishment. DDSR algorithm also reduced the average number of packet delivery time and routing overhead. The reason is route re-establishment takes longer time than keeping the route still usable.
Active DSR Reduces miss rates that lead to significant savings for the flooding in a large network. The flooding rate is also reduced so that significantly reduced the routing overhead.
MEDSR Decreased per packet energy consumption to deliver more useful data packet compared to DSR. The major limitation of MEDSR protocol is that the data packet travels larger number of hops compared to DSR.
EDSR Greater of throughput and less of malicious nodes in network compared to DSR.

Table 1: *Features of DSR's Extension Protocol*

REFERENCES

Alilou, M., & Dehghan, M. (2005). Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks. *Proceeding of World Academy of Science, Engineering and Technology,* **5**, 38-40.

He, Y., & Raghavendra, C. S.(2002) Active Packets Improve Dynamic Source Routing for Ad-hoc Networks.

Jaddi, F., & Paillassa, B. (2005). An Adaptive Hierarchical Extension of DSR: The Cluster Source Routing. *Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05).*

Leung, R., Liu, J., Poon, E., Chan, A. C, & Li, B.(2001). MP-DSR : A QoS aware Multi-path Dynamic Source Routing Protocol for Wireless Ad-hoc Networks.

Maity, S., Saha, S., Sahnawaj, S., Saha, B.K., & Bhunia, C. T. (2008).Pre-emptive Dynamic Source Routing: A Repaired Backup, Approach and Stability Based DSR with Multiple Routes. *Journal of Computing and Information Technology – CIT,* 2, 91-99.

Naski, S. (2004). Performance of Ad Hoc Routing Protocols: Characteristics and Comparison. *Seminar on Internetworking*.

P´erez, M. A. O., Olivera,V. M., & Merino, L. R. (2005). Abbreviated Dynamic Source Routing: Source Routing with Non-Unique Network Identifiers. *Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05).*

Raghavan, V. N., Labbai, T. P. M., Bhalaji, N., & Kesavan, S. (2006). Extended Dynamic Source Routing Protocol for the Non Co-Operating Nodes in Mobile ad hoc Networks. *Proceeding of World Academy of Science, Engineering and Technology* ,16, 249-254.

Rawat, A., Vyavahare, P. D., & Ramani, A. K. (2006). Enhanced DSR with secured multi-path route discovery and concurrent data transmission, 612-613.

Sjaugi, M. F., Othman, M., & A.Rasid,M. F. (2008). A New Distance Based Route Maintenance Strategy for Dynamic Source Routing Protocol. *Journal of Computer Science*, 172-180.

Tarique, M., & Islam, R. (2007). Minimum Energy Dynamic Source Routing Protocol for Mobile Ad Hoc Networks.

IJCSNS International Journal of Computer Science and Network Security, 7, 304-310.

Tarique, M., Tepe, K.E., & Naserian, M. (2005). Hierarchical Dynamic Source Routing: Passive Forwarding Node Selection for Wireless Ad Hoc Networks, 73-78.

Wang, L., Zhang, L., Shu, Y., & Dong, M (2000). Multipath Source Routing in Wireless Ad Hoc Networks, 479-483.

Wei, W., & Zakhor, A.(2004) Robust Multipath Source Routing Protocol (RMPSR) for Video Communication over Wireless Ad Hoc Networks.

An, H.-Y., Zhong, L., Lu, X.-C., & Peng, W. (2005). A Cluster-Based Multipath Dynamic Source Routing in MANET, 369-376.