Source Routing-based Multicast Protocol for Mobile Ad hoc Networks

Hasnaa Moustafa and Houda Labiod

Ecole Nationale Supérieure des Télécommunication
INFRES Department – 46 rue Barrault – 75634 Paris Cedex 13
Tel: +33 (0)1.45.81.74.36 Fax: +33(0)1.45.81.31.19
Email: labiod@enst.fr , moustafa@enst.fr

Abstract

Routing in mobile ad hoc networks is an important research topic where various mechanisms have been already proposed concerning this issue. In this paper, we focus on one critical issue that is multicast routing. Actually, most existing multicast protocols face lot of problems in tree maintenance and frequent reconfiguration when link failures occur. In this context, we propose a new on-demand multicast routing protocol, named Source Routing-based Multicast Protocol (SRMP). It constructs a mesh to connect group members, providing robustness against mobility. SRMP uses the concept of “forwarding group” nodes during its mesh construction. The mechanism of source routing proposed in DSR protocol, is also applied in a modified manner. We evaluated the performance of SRMP via simulations carried out in ns2. A comparison with DSR shows that SRMP provides higher throughput in intermediate mobility, although it exhibits a little impact on the delay without affecting the network overload.

Keywords: multicast routing, mobile ad hoc networks, source-routing concept, forwarding-group concept, link state prediction, energy-conserving.

I. Introduction

The advent of ubiquitous computing and the proliferation of portable computing devices have raised the importance of mobile and wireless networking. Recently, there has been a tremendous interest in broadband wireless access systems, including wireless local area networks (WLAN), broadband wireless access and wireless personal area networks (WPAN). This domain is a subject of a huge research and many standardization activities are undertaken throughout the world, in many 3G/4G related study committees like ITU-R, ETSI BRAN and IEEE 802. Research prototyping is currently underway at many research academic and industrial institutions [1].

In the context of these systems, mobile ad hoc networks (MANETs) have appeared with specific configurations. They provide a powerful paradigm for modeling open self-configuring wireless networks and seem so appropriate to use in the fourth generation of mobile networks. A MANET is an autonomous collection of mobile nodes forming a dynamic network and communicating over wireless links. Users are allowed to communicate with each other in a temporary manner with no centralized administration and in a dynamic topology that changes frequently. Due to the limited propagation range of wireless environment, routes in ad hoc networks are multihop, and mobile nodes in this network dynamically establish routing among themselves to form their own network “on the fly” [2]. Each participating node acts both as a host and a router and must therefore be willing to forward packets for other nodes. Nodes in such a network move arbitrarily, thus network topology changes frequently, unpredictably, and may consist of unidirectional links as well as bi-directional links. Moreover, wireless channel bandwidth is limited. The scarce bandwidth decreases even further due to the effects of signal interference, and channel fading. Network hosts of ad hoc networks such as laptops and personal digital assistants operate on constrained battery power, which will eventually be exhausted, and limited CPU and storage capacity. MANETs strictly depend on radio links. Actually, a wireless link is the most variable and unpredictable communication channel. In addition, ad hoc networks are vulnerable to attacks and have limited physical security. The increased possibility of eavesdropping, spoofing and denial-of-service attacks should be carefully considered. Because ad hoc networks do not typically allow the same aggregation techniques that are available to standard Internet routing protocols, they are vulnerable to scalability problems. These drawbacks lead to define a set of underlying assumptions and performance concerns for protocol design.

Ad hoc networks do not rely on any pre-established infrastructure and can therefore be deployed in places with no infrastructure. This is useful in
disaster recovery situations and places with non-existing or damaged communication infrastructure where rapid deployment of a communication network is needed [3]. Ad hoc networks can also be useful in conferences where people participating in the conference can form a temporary network without engaging the services of any pre-existing network [4]. Routing in mobile ad hoc networks is a significant research topic where various mechanisms have been already proposed concerning this issue. In fact, conventional routing protocols are not well suited in ad hoc environment for several reasons. Firstly, they are designed for static topology, which is not the case in ad hoc network. Secondly, they are highly dependent on periodic control messages; this is in contradiction with resource-limited ad hoc environment. Moreover, classical protocols try to maintain routes to all reachable destinations, which wastes resources. Another limitation comes from the use of bi-directional links, which is not always the case in ad hoc environment. Actually, there is a need for new routing protocols, adapting to the dynamic topology and the wireless links' limitations. Routing protocols in such networks should provide a set of features including [4]: distributed operation, loop freedom, on-demand based operation, unidirectional link support, power conservation, multiple routes, efficiency, scalability, security and quality of service support. However, none of the proposed protocols have all the above desired properties, but these protocols are still under development and are being probably enhanced and extended with more functionality. Until now, no standard has been adopted and many critical issues remain to be solved.

The multicast concept for packet-oriented networks has been widely studied during the past years due to the huge increase of the number of bandwidth-intensive multicast-based applications [5] in conjunction with the popular grow of Internet applications. The advantage of multicast communication is its efficient saving in bandwidth and network resources since the sender can transmit its data with a single transmission to a group of receivers [6]. Nowadays, typical ad hoc environments offer an excellent deployment field for such applications because network nodes may work in groups to carry out a given task. By extending the multicast technology to the ad hoc domain, applications such as videoconferencing, distributed games and computer supported collaborative work can be provided. In this paper, our work focuses on one critical issue in MANETs that is multicast routing. Indeed, the advantages mainly expected are providing efficient saving in bandwidth, reducing communication cost, supplying efficient data delivery with highly unpredictable nodes' mobility, and supporting dynamic topology with unreliable wireless links. Until now, only a few multicast routing protocols have been proposed. Consequently, we propose a novel multicast routing protocol. Our scheme named Source Routing-based Multicast Protocol (SRMP) operates in a loop-free manner and attempts to minimize both routing and storage overhead in order to provide efficiently robustness to host mobility, adaptability to wireless channel fluctuations, and optimization of network resources use. It applies the source routing mechanism defined by the Dynamic Source Routing (DSR) unicast protocol [7] to avoid channel overhead and improve scalability. SRMP is a mesh-based, instead of tree-based, protocol that provides richer connectivity. It outperforms other multicast protocols by providing available stable paths based on future prediction for links’ states. These paths also guarantee nodes stability with respect to their neighbors, strong connectivity between nodes, and higher battery life.

This paper is organized as follows. Section II provides a brief survey on routing protocols in MANETs, pointing out the advantages of multicast routing in the context of multihop wireless communications, and stating the most recent protocols proposed by the Internet Engineering Task Force (IETF) MANET working group. Section III gives a detailed description of our proposed protocol SRMP. Section IV analyzes our performance results. Finally, section V provides concluding remarks and highlights our future work.

II. Multicast Routing: A Brief Survey

In this section, we briefly describe routing protocols in ad hoc networks. Then, we focus particularly on multicast routing since it is the focal point of the study undertaken in this work.

Many classifications are found in the literature. The first one reflects the existence of three main categories based on the routing strategy. Firstly, there are protocols, which use a proactive approach to find routes between all source-destination pairs regardless of the need of such routes. The main feature of this class consists of keeping continuous up-to-date routing information from each node to each other node in the network. Destination-
Sequence-Distance-Vector (DSDV) protocol [8] is an example of this approach; it comes as an improvement of Distributed Bellman Ford (DBF) protocol [9]. This approach also includes Wireless Routing Protocol (WRP) [10], Global State Routing (GSR) and Fishy State Routing (FSR) protocols [11], which are based on link state algorithms. Landmark Ad hoc Routing (LANMAR) [3], and Optimized Link State (OLSR) [12] protocols recently proposed by the MANET group also fall into this category.

Secondly, there are the reactive (on-demand) routing protocols suggested with the key motivation of reducing routing load. Contrarily to proactive mechanisms, these protocols do not maintain routes to each destination continuously. Instead, they initiate routing procedures on an “on-demand” basis. DSR, Signal Stability Routing (SSR) [13], Associativity Based Routing (ABR) [10], and Temporally Order Routing Algorithm (TORA) [10] are typical on-demand routing protocols.

In addition to the above-mentioned protocols, hybrid protocols combine reactive and proactive characteristics, which enable them to adapt efficiently to the environment evolution. This approach comprises Zone Routing Protocol (ZRP) [14].

Table 1 states the advantages and disadvantages of the main approaches cited above.

<table>
<thead>
<tr>
<th></th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive</td>
<td>Up-to-date routing information</td>
<td>Slow convergence</td>
</tr>
<tr>
<td></td>
<td>Quick establishment of routes</td>
<td>Tendency of creating loops</td>
</tr>
<tr>
<td></td>
<td>Small delay</td>
<td>Large amount of resources needed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Routing information not fully used</td>
</tr>
<tr>
<td>Reactive</td>
<td>Reduction of routing load</td>
<td>Not always up-to-date routes</td>
</tr>
<tr>
<td></td>
<td>Saving Resources</td>
<td>Large delay</td>
</tr>
<tr>
<td></td>
<td>Loop-free</td>
<td>Control traffic and overhead cost</td>
</tr>
<tr>
<td>Hybrid</td>
<td>Scalability</td>
<td>Arbitrary proactive scheme within zones</td>
</tr>
<tr>
<td></td>
<td>Limited search cost</td>
<td>Inter-zone routing latencies</td>
</tr>
<tr>
<td></td>
<td>Up-to-date routing information within zones</td>
<td>More resources for large size zones</td>
</tr>
</tbody>
</table>

Table 1: Proactive vs. reactive vs. hybrid approaches

Routing protocols can be also classified in terms of an architectural view. Most traditional classification contains hierarchical protocols and flat protocols [10]. A third classification identifies two types of mechanisms according to the location characteristic: Physical Location Information (PLI)-based protocols giving approximate location for mobile nodes, and PLI-less protocols.

Multipoint communication has emerged as one of the most research areas in the field of networking. As the technology and popularity of Internet grow, applications, such as video conferencing, that require multicast support are becoming more widespread. Multicast protocols used in static networks as Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), Core Based Trees (CBT), and Protocol Independent Multicast (PIM) do not perform well in wireless ad hoc networks due to the fragile multicast tree structures, which must be readjusted as connectivity changes. Furthermore, multicast trees usually require a global routing substructure such as link state or distance vector. The frequent exchange of routing vectors or link state tables, triggered by continuous topology changes, yields excessive channel and processing overhead. Hence, the tree structures used in static networks must be modified, or a different topology between group members need to be deployed for efficient multicasting in wireless ad hoc networks [15].

To provide efficient multicast routing in MANETs, a different kind of protocols should be designed. These protocols should modify the conventional tree structure, or deploy a different topology between group members [16]. Some technical challenges of multicast routing are as follows [17]: minimizing network load, providing basic support for reliable transmission, designing optimal routes, providing robustness, efficiency, active adaptability, and unlimited mobility. Because of the complexity of multicast routing in ad hoc networks, only a few propositions have been made. Globally, we notice two main categories, tree-based protocols (e.g. MAODV, ABAM, MZR [18], SMBP [19]) and mesh-based protocols (e.g. ODMRP, PatchODMRP). The multicast extension of Ad Hoc On Demand Distance Vector (MAODV) routing protocol [20] uses destination sequence number for each multicast entry requiring a lot of control messages. The On-Demand Multicast Routing
Protocol (ODMRP) [21] is based on a mesh structure for connecting multicast members using the concept of forwarding group nodes. ODMRP uses shortest path as a criteria to select forwarding group nodes, which is not the optimal route in a dynamic network as ad hoc network. PatchODMRP [22] extends the ODMRP providing a more efficient way to deal with small number of multicast sources and high mobility. However, it still considers the shortest path criteria. Associativity-Based Multicast Routing (ABAM) protocol [23] has been advocated to improve routing performance, based on choosing more stable routes. However, this method could not avoid frequent rerouting due to node mobility. Table 2 summarizes the major features of multicast routing protocols.

<table>
<thead>
<tr>
<th>Protocol Parameter</th>
<th>ODMRP</th>
<th>PatchODMRP</th>
<th>MAODV</th>
<th>ABAM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast delivery (Configuration)</td>
<td>Mesh</td>
<td>Mesh</td>
<td>Shared-Tree</td>
<td>Source-based Tree</td>
</tr>
<tr>
<td>Routing Approach</td>
<td>On-demand</td>
<td>On-demand</td>
<td>On-demand</td>
<td>On-demand</td>
</tr>
<tr>
<td>Dependency on unicast routing</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Periodic Flooding</td>
<td>Join-Query</td>
<td>Join Request</td>
<td>Route Request</td>
<td>No</td>
</tr>
<tr>
<td>Control overhead</td>
<td>At gp. Formation and periodic flood</td>
<td>At gp. formation only</td>
<td>At tree construction and maintenance</td>
<td>At tree construction and repair</td>
</tr>
<tr>
<td>Routing philosophy</td>
<td>Flat</td>
<td>Flat</td>
<td>Flat</td>
<td>Flat</td>
</tr>
<tr>
<td>Routing metric</td>
<td>Shortest path</td>
<td>Shortest path</td>
<td>Freshest and shortest path</td>
<td>Tree and link longevity</td>
</tr>
<tr>
<td>Loop-free</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 2: Comparison of multicast protocols

Obviously, multicast routing is a young research domain, no standard has been adopted yet and many issues have to be addressed and more studies are needed. Actually, most existing multicast protocols face several problems in tree maintenance and frequent reconfiguration when link failures occur. These protocols depend on upstream and downstream nodes requiring storage and control overhead. Moreover, some protocols consider the shortest path as a criterion for path selection, which is not usually suitable to the high and unpredictable variation of the topology. In this context, we propose a new on-demand multicast routing protocol, named Source Routing-based Multicast Protocol (SRMP). This protocol constructs a mesh to connect group members thus providing robustness against mobility. Multicast routes and group memberships are obtained on-demand to use efficiently network resources, avoiding channel overhead and improving scalability.

III. SRMP

This section gives an overview of SRMP. The selection criteria used in mesh establishment is pointed out, showing the metrics used to select Forwarding Group (FG) nodes. The used data structures are presented, and the protocol operation is described and illustrated through an example.

1. Protocol Overview

Our protocol named SRMP is a mesh-based multicast routing protocol [24]. A mesh structure (arbitrary subnetwork) is established on-demand to connect group members, providing richer connectivity among multicast members. A multicast mesh is a subset of the network topology that provides at least one path from each source to each receiver in the multicast group. By building a mesh, packets can be delivered to multicast receivers in the case of node movements and topology changes; routers are allowed to accept unique packets coming from any neighbor in the mesh. In addition, drawbacks of multicast trees can be avoided (ex, intermittent connectivity, traffic concentration, frequent tree reconfiguration, non-shortest path in a shared tree).

The mechanism of source routing proposed in DSR unicast protocol is applied, in a modified manner. Available paths are provided through future prediction for links’ states.

Route selection takes place through establishing a multicast mesh, started at the multicast receivers, for each multicast session. The concept of FG nodes is used during mesh establishment. The FG is a set of selected nodes responsible for forwarding multicast data between any member pairs [15].
This scheme can be viewed as “limited scope” flooding within a properly selected forwarding set.

This protocol investigates the routing problem in MANETs through considering a distinctive approach. Basically, it addresses three issues in this problem: path availability, power conserving, and nodes’ strong connectivity.

2. FG Nodes Selection

The key challenge in efficient multicasting is the choice of FG nodes and how to elect and maintain them. SRMP achieves a compromise between the size of the selected nodes, the availability and stability of the selected paths. SRMP applies efficient FG nodes selection criteria through defining four metrics: association stability, link signal strength, battery life, and link availability.

2.1 Association Stability

This metric measures how long the node is stable with respect to each neighbor. It has been first introduced in ABR protocol [10], and is known as the degree of association stability. Association stability is calculated by each node with respect to each neighbor through the use of associativity ticks field stored in the node’s Neighbor_Stability_Table. It is incremented each time the node receives a beacon indicating neighbor’s existence. A node is considered stable with respect to a neighbor, when the accumulated associativity ticks value corresponding to this neighbor fulfills a predefined threshold.

2.2 Link Signal Strength

This metric measures the signal strength between each node and each of its neighbors indicating connectivity strength. It is used as a part of SSR unicast routing protocol [13]. SRMP uses this metric to select links that offer stronger connectivity between nodes. Signal strength is calculated according to the level of strength the beacon is received, where it is classified as weak or strong. In fact, classification is done through comparing the level of strength of the received beacon with a predefined threshold.

2.3 Battery Life

This metric periodically calculates the current battery power, which is a decreasing function of time and processed packets. It biases the protocol towards choosing a channel that tends to power conserving. Paths with higher battery life, indicating less power consumption, are only selected. The node is considered as possessing high battery life, as long as its battery life counter (see Formula 2.1) fulfills a predefined threshold.

\[
B_p(t) = B_p(\text{current}) - [PC_{gp} + PC_{rp} + PC_{fp} + K] \quad (1)
\]
- \(B_p(t)\): Battery power at time \(t\)
- \(B_p(\text{current})\): Current battery power (Initially, \(B_p(\text{current}) = B_p(0)\))
- \(PC_{gp}\): Total power consumed for each generated packet (including processing and transmission)
- \(PC_{rp}\): Total power consumed for each received packet (including reception and processing)
- \(PC_{fp}\): Total power consumed for each forwarded packet (including reception, processing and transmission)
- \(K\): Power consumed by the node itself (equipment)

2.4 Link Availability

Path availability allows the protocol to distinguish between available and unavailable paths, in terms of the radio quality of each link constituting the path. SRMP uses a link availability estimation metric during path selection, based on a probabilistic model for future availability of the path. We use the prediction-based link availability estimation introduced in [11].

3. Data Structures

To enable SRMP routing, we define the following data structures:

- **Neighbor_Stability_Table** that gathers continuous node-neighbor information,
- **Multicast_Message_Duplication_Table** that identifies each received Join-request or data packet,
- **Multicast_Routing_Cache** that stores all possible routes from each node to each multicast group,
• *Receiver_Multicast_Routing_Table* maintained at each receiver for each multicast group, and stores the used route between each receiver and each source.

<table>
<thead>
<tr>
<th>Neighbor</th>
<th>Type</th>
<th>Associativity ticks</th>
<th>Signal strength</th>
<th>Link availability</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 3: Neighbor_Stability_Table

<table>
<thead>
<tr>
<th>Source ID</th>
<th>Sequence number</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4: Multicast_Message_Duplication_Table

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Source ID</th>
<th>Route to source</th>
<th>Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5: Receiver_Multicast_Routing_Table

<table>
<thead>
<tr>
<th>Group ID</th>
<th>Type</th>
<th>Route to receiver</th>
<th>Timer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6: Multicast_Routing_Cache

4. Operation

Similar to the operation of on-demand routing protocols, a request phase and a reply phase comprise the protocol. The request phase invokes a route discovery process to find routes to reach the multicast group. Different routes to the multicast group are setup during the reply phase through FG nodes selection and mesh construction.

The following sections describe the request phase, reply phase, FG nodes selection, and data transmission/forwarding through the constructed mesh.

4.1 Request Phase

This phase starts when a source node, which is not a group member, wishes to join the group. It invokes a route discovery procedure towards the multicast group, through broadcasting a *Join-request* packet to neighbors. This packet contains the ID of the source node in a *Source ID* field, the multicast group ID in a *Destination ID* field, and a *Sequence number* field set by the source node. To eliminate the possibility of receiving multiple copies for a *Join-request*, each node receiving a *Join-request* detects duplication through checking its multicast message duplication table.

This phase is considered a modified form of the DSR route discovery process. The major mismatch arises in the means of applying the source routing concept, which accumulates in the *Join-reply* packet during the reply phase instead of accumulating in the request phase. Thus, we eliminate channel and routing overhead.

4.2 Reply Phase and Mesh Construction

Initially, a multicast receiver initiates the reply phase. A multicast receiver, when receiving a *Join-request* packet, first checks for stability among its neighbors including associativity ticks, signal strength, and link availability. Battery life is also checked considering consumed power needed to transmit to each neighbor. When these metrics satisfy predefined thresholds, the receiver selects the neighbor as FG node and sets it as a member in the *Neighbor_Stability_Table*. The receiver then sends a *Join-reply* packet to this FG node, storing the multicast group ID in a *Source ID* field and the ID of the requesting node in a *Destination ID* field. A source route also accumulates, during *Join-reply* propagation, in a *Route record* field in the packet.

An FG node, receiving a *Join-reply*, first creates an entry to the multicast group in its *Multicast_Routing_Cache*, setting its state as FG node and copying the reversed accumulated route in the received *Join-reply*. It then performs same previous steps for selecting FG nodes among neighbors. This process continues until reaching the source, constructing a mesh of FG nodes, which connect group members.

A source receiving a *Join-reply* packet creates an entry to the multicast group in its *Multicast_Routing_Cache*. More than one *Join-reply* may be
received by the source for the same multicast group. Hence, multiple routes can be stored for the same multicast group.

After mesh creation, new Join-request packets may receive replies from any FG member node, having unexpired routes to the requested multicast group. In this case, the FG node sends the Join-reply, following the same previous selection among neighbors.

4.3 Data Transmission

The shortest path route is selected to transmit data. If more than one shortest path routes are found, the freshest route is selected. Data packets carry in their headers the selected route indicating the sequence of hops to be followed.

Each FG node receiving a data packet forwards this packet, if it stores in its cache at least one valid route towards the multicast group and the packet is not duplicated. This leads to an attractive feature in SRMP, preventing packets transmission through stale routes and minimizing traffic overhead. The process continues until reaching all multicast receivers.

A multicast receiver, receiving a data packet for the first time, creates an entry in its Receiver_Multicast_Routing_Table. To guarantee data transmission to all multicast receivers, nodes duplicate transmission if the selected route leads directly to the multicast group. We define duplication in transmission, as selecting one more route following same previous criteria and transmitting data to both routes.

We give an example, illustrating SRMP operation. Consider the ad hoc network shown in Figure 1. Node (S) is the multicast source wishing to join the group, and (R₁, R₂) are the multicast receivers of the group.

![Figure 1: Join-request generation by S](image1)

![Figure 2: Join-reply phase](image2)
First, S broadcasts *Join-request* packet discovering routes to the multicast group (see Figure 1). Meanwhile, duplication of *Join-request* is detected and discarded.

Figure 2(a) and Figure 2(b) show respectively the reply phase from receivers (R₁, R₂) to the source S, constructing the mesh and selecting FG nodes following SRMP selection criteria. During *Join-reply* propagation, *Multicast_Routing_Cache* entries are created or refreshed at each node.

Figure 3 shows the created mesh with nodes X and Y selected as FG nodes.

5. Maintenance

Route maintenance concerns with reporting and recovering routing problems, keeping the lifetime of a route as long as possible. For this purpose, SRMP addresses four mechanisms providing multicast mesh refreshment: link breaks detection and repair, continuous node-neighbor information, and pruning allowing any node to leave the group. Two new messages are introduced: the *Multicast-RERR* message (section 5.3), and the *Leave Group* message (section 5.4).

5.1 Neighbor Existence Mechanism

SRMP uses MAC layer beacons to provide each node with neighbors’ existence information. Upon reception of neighbors’ beacons, creating or updating *Neighbor_Stability_Table* entries takes place via incrementing the associativity ticks, and setting the signal strength according to the level of strength the beacon is received. In addition, link availability is updated by continuous prediction for links’ availability towards neighbors. If no beacons are received by a node from a neighbor up to a certain period of time, the node indicates neighbor's movement and updates its stability table fields towards it.

5.2 Mesh Refreshment Mechanism

It follows a simple mechanism making use of data packets propagation and requiring no extra control overhead. Each time the source transmits a data packet, it updates in its cache the timer of the used route. Typically, an FG node forwarding this packet scans the packet header, and refreshes in its cache the corresponding route entry timer. Furthermore, a multicast receiver scans the header of each received data packet, refreshing its corresponding table entry timer to the source. Periodically, each node checks its timers and purges out expired multicast group entries, preventing stale routes storage. In addition, it checks its neighbor table, deleting from its cache routes to multicast groups for which it possesses no more members.

5.3 Link Repair Mechanism

SRMP reacts to links’ failures on-demand, it detects failures during data transmission through the use of MAC layer support. In this case, two mechanisms are addressed: maintaining routes when a link fails between two FG nodes, and maintaining routes when a link fails between a multicast receiver and an FG node. In fact, mesh reconfigurations are not needed if the stability characteristics together with high battery life paths are valid through out the lifetime of the multicast communications.

When links’ failures occur between two FG nodes, the node detecting failure reports it to the original source following the same procedure of link failure recovery in DSR protocol. First, it generates a *Multicast-RERR* packet indicating the broken link in a *Broken link* field in this packet. Then, it deletes from its cache any routes containing the broken link. Nodes on the way to the source, receiving this packet, in turn clean their caches from all routes containing the broken link.
When Links fail between an FG node and a multicast receiver, an alternative approach is applied. Simply, the FG node detecting failure deletes the receiver membership from its Neighbor_Stability_Table. When the FG node possesses no more members for the multicast group, it deletes routes to this group from its cache and sends to all its neighbors a Multicast-RERR packet reporting the failure. The Broken link field in this packet stores the link between the failure detector FG node and the multicast group. Each neighbor, receiving this packet, cleans its cache from routes containing the broken link. The process is repeated until all member nodes in the mesh are visited.

5.4 Pruning Mechanism

SRMP employs an effective pruning mechanism allowing a member node to leave the multicast session. It deals with two cases: FG node pruning, and multicast receiver pruning. A multicast source wishing to leave a multicast group simply stops transmitting data to this group, deleting from its cache entries concerning this group.

Typically, a multicast receiver wishing to leave a multicast group sends a Leave Group message to its member neighbors, deleting from its table all entries corresponding to this group. The Leave Group message carries the ID of the multicast session in a Multicast group ID field, and the ID of the member neighbor to which the message is sent in a Neighbor ID field. The neighbor node, receiving this message, cancels in its turn the receiver membership from its Neighbor_Stability_Table. When this node has no more members for a multicast group, it sends in its turn a Multicast-RERR message to its member neighbors following previous procedure in link failure.

Furthermore, an FG node wishing to leave a multicast group starts by sending a Leave Group message to its member neighbors, deleting from its cache all multicast group entries. Each neighbor receiving this message cancels in its turn the FG node membership from its Neighbor_Stability_Table. It deletes routes containing this node from its cache, and sends Multicast-RERR message to its member neighbors following the previous procedure of link failure. The Broken link field in this message stores the FG node, which has left.

One significant characteristic in our protocol is its reactive approach in discovering routes and detecting link failures. In comparison to other existing protocols, it guarantees nodes’ stability and strong connectivity with respect to neighbors, offering much longer route lifetime. The problems of the tree structure are significantly reduced in SRMP through constructing a mesh topology, achieving minimized flooding scope thanks to applying the FG node concept. Through employing an efficient mesh refreshment mechanism; introducing no extra control overhead SRMP outperforms other mesh-based protocols as ODMRP, which invokes periodical requests/reply to refresh its mesh. Additionally, via the efficient repairing and pruning mechanisms, SRMP achieves superiority over ODMRP that employs no special mechanisms.

IV. Performance Evaluation

IV.1 Simulation Model

Network Simulator2 is used to study the performance of SRMP. It is a discrete event simulator developed at Berkeley University targeted at networking research [25]. The overall goal of our simulation study is to analyze the behavior of our protocol under a range of various mobility scenarios. Our simulations were run using a manet composed of 7 nodes moving over a square 500m x 500m flat space.

<table>
<thead>
<tr>
<th>Topography</th>
<th>500m x 500m</th>
</tr>
</thead>
<tbody>
<tr>
<td># of nodes</td>
<td>7</td>
</tr>
<tr>
<td>Max. speed</td>
<td>10 m/s</td>
</tr>
<tr>
<td>Traffic type</td>
<td>CBR</td>
</tr>
<tr>
<td># of traffic sources</td>
<td>3</td>
</tr>
<tr>
<td>Packet size</td>
<td>512 bytes</td>
</tr>
<tr>
<td>Emission rate</td>
<td>4 pkts/sec</td>
</tr>
<tr>
<td>Pause time</td>
<td>[0,500]</td>
</tr>
<tr>
<td>Node range</td>
<td>250 m</td>
</tr>
<tr>
<td>Simulation time</td>
<td>500 sec</td>
</tr>
<tr>
<td>Max. Time between request</td>
<td>10.0 sec</td>
</tr>
<tr>
<td>Waiting time for request</td>
<td>0.5 sec</td>
</tr>
<tr>
<td>Waiting time for reply</td>
<td>2 sec</td>
</tr>
<tr>
<td>Neighbor validity time</td>
<td>2.7 sec</td>
</tr>
<tr>
<td>Neighbor table update interval</td>
<td>3.0 sec</td>
</tr>
</tbody>
</table>

(a) Network configuration                              (b) SRMP parameters

Table 7: Simulation Model Parameters
Table 7(a) and (b) show the used parameters. The radio and MAC models are described in [25]. The movement scenario files used for each simulation are characterized by a pause time. 15 different movement patterns are generated for 6 various pause times.

### IV.2 Simulation Results

As a first step, we choose to simulate SRMP unicast communication without including the full mesh reconfiguration or the pruning mechanism in order to have a preliminary estimation on the overall performance of a light version of the protocol. We make a comparison between SRMP and DSR results. We used the following main performance metrics: average end-to-end delay, throughput, dropped packets, and routing overhead. The results are shown in the following section.

#### A. Average End-to-End Delay

Figure 4 shows the average end-to-end delay as a function of the mobility scenario. In this figure, results for the protocol SRMP are compared with those of DSR. This delay is calculated only for the data packets that have been successfully received. We can see that the delay has nearly the same behavior for both protocols at all different pause times. SRMP causes a slight increase in delay over DSR. This increase constitutes approximately 2.5% at pause time 0 (very high mobility) and reaches 6%, maximum increase, for pause time 300 (nearly low mobility). This difference is reduced when the network becomes stable; in this case the two protocols show nearly the same behavior since routes become stable. It is clear that SRMP has no bad impact on the delay compared to DSR thanks to the applied nodes’ selection and mesh construction mechanisms, which decrease congestion and construct more minimum hops paths.

#### B. Throughput

A comparison based on the throughput is depicted in Figure 5. The throughput is determined by the ratio of the number of data packets actually delivered to the destination versus the number of data packets supposed to be received. This number presents the effectiveness of the protocol. We can see that the two protocols point up the same behavior in all mobility cases. At low mobility, SRMP provides nearly same throughput as DSR because of its rigid mesh structure by means of selecting stable paths to form the mesh. At high mobility, both protocols exhibit a decrease in throughput. SRMP shows an 18% decrease in throughput with respect to DSR. This result confirms the expected behavior with the increased packet loss rate arising from link breakage and mesh reconfiguration requirements, which is not fully simulated in SRMP. In fact, congestion rate increases causing the request and reply messages to be delayed or even lost. Results are slightly in favor of DSR with nearly the same performance in low and intermediate mobility environment and we expect better performance when all SRMP features are included.
C. Dropped Packets

Figure 6 shows the effect of SRMP and DSR on the number of dropped packets. It is obvious that DSR has a very weak impact on packets drop for high mobility, while SRMP has more impact on packets drop in this case. This refers to the fact that no complete mesh reconfiguration is implemented in SRMP invoking the need for re-transmission. When link failure occurs, queue congestion is increased causing more packets drop. In contrast, DSR applies full maintenance mechanism that recovers quickly link failure and avoids large number of drops. At intermediate mobility, packets drop decreases gradually in SRMP with pause time increase until it outperforms DSR. We can explain this by the fact that the link breakage probability decreases at the same time the stability features in SRMP allows it to outperform DSR.

D. Routing Overhead

In this section, the control overhead comparison is subsequently illustrated. We observe a significant difference between SRMP and DSR in terms of control packets generated during simulation for medium and low mobility (Figure 7).

Thanks to the on-demand mesh structure of SRMP, results emphasize a very small control overhead. Furthermore, the effective node selection mechanism in SRMP, where packets are generated only to certain nodes,
and the fact of selecting more stable paths decrease the probability of link failure and the need to send more routing packets to recover this failure.

Figure 8: Bytes overhead as a function of pause time

Concerning the total number of control bytes overhead generated, we can clearly see that SRMP verges more to DSR in the case of high mobility (Figure 8), this is due to the source routing concept used in both protocols that adds a number of bytes in each packet. It is obvious that, SRMP outperforms DSR in bytes overhead for intermediate and low mobility. This comes from the fact that SRMP accumulates and sends source routes during reply phase, thus to a smaller number of nodes. On the contrary DSR accumulates the source route during route request broadcast, thus consuming more overhead bytes.

Our performance investigation is considered as a first phase to demonstrate the correct operation of SRMP. The preliminary results of unicast operation are very encouraging and motivate to continue to implement the other functionalities making benefit of their strengths. Our goal is to analyze fully and more precisely the overall protocol as a function of nodes mobility level and network loads in order to assess its relative might and weakness.

V. Conclusion

The field of ad hoc mobile networks is rapidly growing and changing and there are still many challenges that need to be met. We notice that the lack of standards in this area of study leads to several works and propositions. Moreover, since ad hoc networking is an emerging concept in computer communications, multicast routing is considered as one critical issue.

In this paper, we focus on multicast routing. Routing requirements are reviewed. Some existing protocols and particularly in multicast domain are cited. Their advantages and limitations are illustrated. Our aim in this study is to present a new on-demand multicast routing approach, providing enhancements over other existing strategies.

Our proposed protocol, SRMP, applies on-demand multicast route construction and membership maintenance, avoiding periodic route construction. It provides some key advantages: robustness and richer connectivity, low channel overhead, maintenance and exploitation of multiple redundant paths, and stable paths with future links’ states prediction. Thanks to applying the FG nodes concept, minimized flooding scope is achieved. By the use of FG nodes and applying the on-demand routing technique, SRMP reduces channel and storage overhead thus improving performance and scalability.

Some relevant enhancements are introduced in SRMP to overcome some drawbacks of other protocols as ODMRP. Instead of using the shortest path criterion in route selection procedure, SRMP uses more effective criteria in the choice of FG nodes regarding paths stability and link availability based on future prediction for links’ states. Thus, it guarantees reliable delivery together with less communication overhead and end-to-end delay. Furthermore, SRMP guarantees loop freedom and fewer overheads in maintaining next hop information, thanks to source routing approach. Other significant strengths of this protocol include higher battery life paths tending to power conserving, route maintenance and pruning capability.

SRMP has shown no bad impact on the delay compared to DSR, thanks to nodes selection and mesh construction. Also, SRMP reduces the amount of control overhead. Furthermore, it enhances the throughput at intermediate and low mobility cases. We plan to complete the routing protocol implementation adding multicast capabilities and integrating the full maintenance procedures. Simulation of our protocol is in progress, the
results will be reported based on making a performance comparison between SRMP and multicast protocols such as ODMRP and MAODV.

References

Biography

Hasnaa Moustafa (moustafa@enst.fr)

Attended high school in Alexandria - Egypt, and graduated from the Arab Academy for Science & Technology (AAST) with a BS degree in computer Engineering 1997. While working as a Teaching Assistant (TA) at AAST 1997-2000, she completed her MSC degree in the area of research “Traffic Control in ATM Networks”. In year 2000-2001, she finished her Diplôme d’étude approfondies (DEA) at Paris in the area of research “Routing Protocols in Mobile Ad hoc Networks”. Now started her PhD studies at ENST – Paris (INFRES Department), supervised by Dr. Houda Labiod. Her research domain concerns routing in mobile ad hoc networks, focusing now on Multicast Routing.

Houda Labiod (labiod@enst.fr)

Obtained her Ph.D in Network and Computer Science from the University of Versailles, France, in 1998. She worked at Eurecom Institute (1998-2000) as an Assistant professor. She is currently an Assistant Professor at the Computer Science and Networks department of ENST. Her research interests include error control mechanisms in mobile networks, multicast and quality of service routing in mobile ad hoc networks, and security in WLANs and 4G networks.