A Reactive Wireless Mesh Network Architecture

Bachar Wehbi, Anis Laouiti and Ana Cavalli

Insitut TELECOM, TELECOM & Management SudParis, CNRS SAMOVAR
{bachar.wehbi, anis.laouiti, ana.cavalli}@it-sudparis.eu

Abstract. The future of wireless networks evolves toward more simple ways for users to get connected while on the move. In this perspective, Wireless Mesh Networks constitute one of the key technologies for new generation wireless networks. In this paper we present a reactive solution for routing and client management in an infrastructure-based wireless mesh network. The solution is based on DYMO[1]/AODV adhoc routing protocol; it performs on-demand path setup for clients and supports their mobility by introducing a light mechanism. Our solution is designed to minimize memory and bandwidth overhead by exchanging only mandatory information for client management and route establishment.

Keywords : *Mesh network, client management, wireless, DYMO/AODV.*

1 Introduction

Wireless mesh networks [2] are flexible and self-organized networks composed of a set of nodes equipped with wireless communication capabilities. Communications in a wireless mesh network are multi-hop where communicating nodes may not be in their direct radio range and rely on the cooperation of intermediate nodes to establish end-to-end routes.

Wireless mesh networks can be classified into infrastructure and infrastructureless based networks according to the capabilities of end user devices. Infrastructureless mesh networks are one-tier network architecture where user devices are part of the routing architecture as they have routing capabilities to relay packets on behalf of other nodes. Infrastructure based mesh networks, which are the focus of this work, are two-tier network architecture composed of a backbone of interconnected mesh routers. A mesh router may be equipped with additional wireless card functioning as an *Access Point* to offer network connectivity for user devices. Mesh routers are responsible for the routing function along with providing network access to user devices. Those are simple clients in the architecture and therefore have no special routing capabilities. Figure 1 illustrates a basic infrastructure based wireless mesh network.

Wireless mesh networks have been the focus of many research studies in the last decade. Most of the proposed solutions focus on routing on the mesh backbone, on capacity estimation of mesh networks and on channel allocation algorithms to exploit multi-channel capabilities [1, 5, 10].

[1] DYMO is the new version of the well known AODV routing protocol.

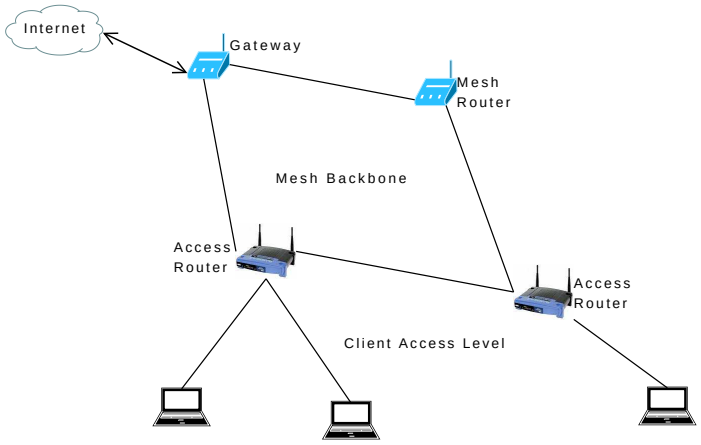

Fig. 1. Wireless Mesh network architecture.

We are interested in designing a wireless mesh architecture that serves for client-to-client and internet communications. The architecture must support client mobility while maintaining low traffic overhead. In addition, the solution should require no modification to client nodes. A client equipped with from the shelf wireless card should take full advantage of the network.

Our approach is based on a reactive mesh architecture in both routing and client management. Mesh routers are not required to keep track of all client nodes in the network. Each mesh router on the communication path involving client nodes maintains a list of these nodes. This partial client information base reduces memory and traffic consumption. We extend existing DYMO adhoc routing protocol to efficiently support the client access level of the mesh architecture.

The reminder of the paper is composed as follows: Section 2 describes some related work. Section 3 discusses the system architecture and its different building blocks. Section 4 concludes the paper.

2 Related Work

The concept of combining the properties of infrastructure and adhoc based networks has been the topic of many recent studies. One approach consisted of building an overlay over adhoc networks in order to improve the performance and increase the scalability of these networks. Other approaches try to exploit the mesh architecture and propose interesting technical solutions.

Hierarchical OLSR (HOLSR) [8] is designed for heterogeneous networks where nodes with different communication capabilities coexist. HOLSR dynamically organizes nodes, all running OLSR, into cluster levels. The objectives of HOLSR are to reduce the amount of exchanged topology control information at different

levels of the hierarchical network topology and to use efficiently high capacity nodes. Our approach differs in that it does not require clients to run any particular routing protocol. The communications are transparent for our clients that think destinations are on the local network. Second, in HOLSR higher level nodes need to add routing entries toward all lower level nodes; this fact will explode their routing tables. Using our approach, a mesh router adds routing entries toward communicating nodes only if it is on the communication path.

For MIT's Roofnet Project [4] mesh clients are directly connected to Ethernet ports on the mesh routers. Network Address Translation is used to mask client addresses from the rest of the network. Contrarily, client nodes in our architecture are mobile; they are connected to the mesh routers using WIFI cards. Client mobility is supported thanks to additional functionalities incorporated into the routing protocol.

The MeshDV [9] protocol uses IP-in-IP encapsulation on end-mesh routers. Intermediate mesh routers see the traffic as being between the end-mesh routers; client communications are transparent for them. Our approach differs from MeshDV in that it requires no encapsulation mechanism. Only intermediate mesh nodes between communicating clients need to know about the communication. This reduces processing complexity implied by IP encapsulation/decapsulation and allows supporting client mobility within the routing protocol. The price is slightly more routing entries on mesh nodes.

The authors in [7] propose an extension to OLSR for mesh networks by using the Association Discovery Protocol (ADP) in order to distribute periodically the *Client Association Base* throughout the mesh network. Each mesh router maintains a Global Association Base recording which client is associated to which mesh router in the entire network.

SMesh [3] presents a mesh system that offers seamless handover to support VoIP and other real-time applications. Seamless handover is achieved by having a group of access routers (called Client Data Group) serving each mobile client. This group of access routers multicasts traffic to the mobile host during handover transitions cutting the handover latency to zero at the cost of higher bandwidth use. The problem of SMesh is that it requires all the access points to work on the same channel; consequently the mobile client can talk to multiple access points simultaneously. This significantly reduces the capacity of the client access level.

3 System Architecture

In this paper we propose a two-tier network architecture composed of a mesh backbone level and a client access level (see fig. 1). The backbone level can be seen as a wireless adhoc network of mesh nodes connected in a multihop manner. Some of the mesh nodes are equipped with additional wireless interface playing the role of access point to offer connectivity to standard WIFI clients; in the following we call these mesh nodes *access routers*. The set of access routers will form an extended basic service set (EBSS) allowing transparent client handover from one access router to another. Clients configure their SSID and join the

network as they do in a classical WLAN. We use a centralized DHCP server that can run on one of the mesh nodes to configure the network with IP addresses. In addition, we rely on DHCP relay agents on each access router to relay DHCP message exchange between the clients and the server. Internet connectivity could be provided by one of the mesh nodes acting as a gateway for the network.

Connectivity in such network requires building routes between different mesh nodes and locating client nodes. An adhoc routing protocol can be used to construct routing tables for mesh nodes. The designed architecture can support proactive or reactive routing protocols. Proactive routing protocols like OLSR have the advantage of providing high knowledge about the network topology. However, the routing control overhead is high as control messages are periodic. The topology on the backbone level is stable as mesh nodes are not mobile in general; therefore there is no need to continue transmitting control messages once we have the topology of the network. Reactive routing protocols like DYMO/AODV have the advantage of low traffic overhead in a low mobility networks. In fact the mesh backbone is stable as mesh routers do not move. On the client access level, client nodes move from one access router to another. After a handover, reactive protocols try to find new routes to the moving nodes if they have active communications while proactive protocols wait until a new route is available in order to be able to contact the moving node. Both reactive and proactive routing protocols have their advantages and drawbacks. In this work we are not comparing them in a mesh topology; on the contrary we are designing a flexible mesh network architecture that can be used with a proactive or a reactive routing protocol. In the rest of this paper we will detail the system architecture assuming a reactive routing protocol is used.

On the backbone level, the routing protocol will build routes between mesh nodes. This routing information is insufficient to find paths between client nodes. To overcome this problem, access routers have to advertise their associated clients to complement the routing information with client locations. We use a reactive approach that consists on advertising client associations only when it is needed. This means when the client is involved in an active communication.

In our architecture, client nodes equipped with standard WIFI devices can take full advantage of the network without any modifications. Client nodes associates with access routers as in a WLAN; the mesh nature of the network is totally transparent for the clients. In order to offer the desired connectivity using the wireless mesh backbone, access routers need to implement the modules illustrated in figure 2. The aim is to link the data link layer client associations with the network layer routing protocol. Each access router runs the following modules:

- Client Management Module
- Routing Module
- DHCP Relay Agent
- ARP Request Handler

A client association with an access router will trigger an entry in the Client Management Module of the access router. The routing protocol consults the

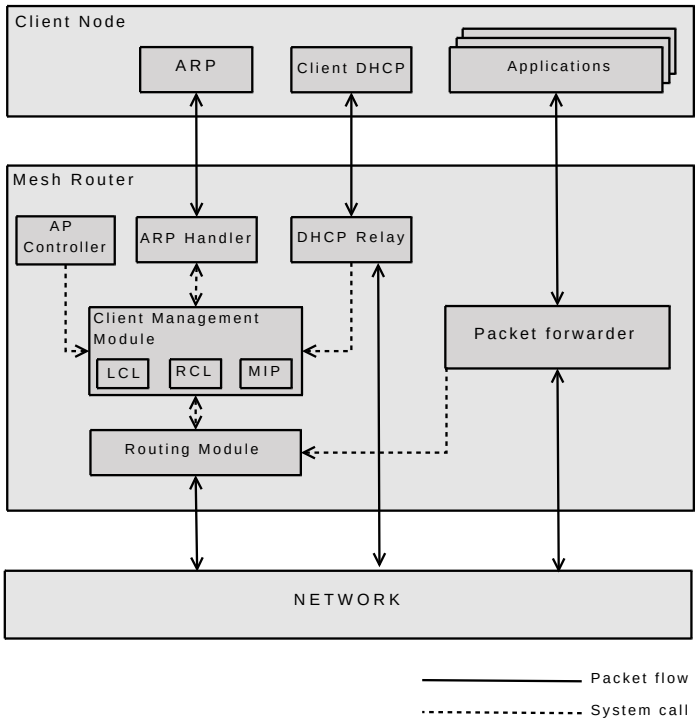

Fig. 2. System architecture: interaction between the different modules

Client Management Module to build and maintain routes toward client nodes. The ARP request handler at the access router will give local client nodes the illusion that the mesh network is a simple broadcast local network. While the DHCP relay agent relays messages between the server and the clients allowing the DHCP service to cover the whole network. We should note here that mesh routers (which doesn't provide client connectivity) run the routing module only. In the following sections we detail each of the mentioned modules before we run through an example illustrating the steps for a communication setup.

3.1 DHCP and MAC to IP Mapping

We propose a simple mechanism to map between IP and MAC addresses of client nodes. In fact, at the client access level, client associations require the MAC addresses of associated nodes whereas routing information at the backbone level requires the IP addresses of communicating clients. For this reason, client nodes IP to MAC addresses mapping is required at the access routers. We changed the IP allocation mechanism of DHCP in order to satisfy this requirement. When the DHCP server receives a request from a client identified by its MAC address, it computes the IP address by applying a hash function to the client's MAC ad-

dress. If the hash function produces an already allocated IP address, the DHCP server selects an IP address from a managed IP range and sends it to the requesting client. Then it generates a message indicating that the client's MAC address is mapped to the offered IP address. Each access router receiving this message, inserts an entry in its *Managed IP* list (MIP) mapping the offered IP to the client's MAC address. This way, all the access routers in the network will have in their MIP the complete list of client nodes that obtained managed IPs. For the rest of the client nodes the mapping between the IP and MAC addresses can be obtained using the hash function.

The DHCP server and the clients exchange messages using local broadcasts, thus the server should exist locally. To overcome this limitation, we let each access router run the DHCP relay agent. The relay agent acts as an intermediate between the server and the clients. It relays the DHCP messages exchange between the client and the server. When the access router (relay agent) receives the DHCP offer message from the server it forwards it to the client and updates its *Local Client Table* (see section 3.2).

3.2 Client Management Module

In order to support the routing module with the required client information to establish and maintain paths between communicating nodes, each access router maintains a *Local Client List* (LCL) containing the list of clients associated to its access point interface and updates it whenever an event occurs (new client association or client disassociation). In addition to the LCL, each access router maintains a *Remote Client List* that contains the list of discovered remote client nodes and their responsible access routers. The RCL list is constructed when the access router receives a routing message containing information about a client that is in communication with a local client (see section 3.4).

LCL holds the list of client nodes associated with the access router. The LCL format is represented in table 1; each entry represents the mapping between the MAC and IP addresses of a given associated client node. This table is updated to reflect the new associations and disassociations of client nodes. In the LCL list, the mapping between the client's IP and MAC addresses is performed as follows: The client node association provides the client's MAC address to the *Client Management Module*. This module checks if the MAC address matches an entry in the *Managed IP* list. If a match exists, the access router inserts in its LCL the mapping between the client's MAC and IP addresses obtained from the MIP list. If no match exists, the access router applies the same hash function used by the DHCP server on the client MAC address to obtain the IP address and inserts the obtained mapping in the LCL list. RCL holds the list of remote clients in communication with local clients. These remote clients are mapped to their responsible access routers. Each entry in the RCL contains the IP address of the remote client node mapped to the IP address of its correspondent access router. The format of RCL is represented in table 2. The LCL and RCL tables, coupled with the routing protocol, allow to discover and to maintain routes between communicating client nodes. If a client node is not involved in any

Local Client List	
Client node IP	**Client node MAC**
Associated client IP 1	Associated client MAC 1
Associated client IP 2	Associated client MAC 2
...	...
Associated client IP n	Associated client MAC n

Table 1. Local Client List Format.

communication, it will appear only in the LCL list of its responsible access router.

Remote Client List	
Remote Client IP	**Remote access router IP**
Client IP 1	Access router IP 1
Client IP 2	Access router IP 2
...	...
Client IP n	Access router IP n'

Table 2. Remote Client List Format.

3.3 ARP Request Handler

The Address Resolution Protocol (ARP) [11] allows the mapping of a network address to a hardware address. In a 802.11 WLAN network, a node can communicate with another node inside the same network only if it knows its MAC address. Given a destination IP address, if its corresponding MAC address mapping is not present in the ARP cache of the client, the ARP module broadcasts an ARP request packet. All the nodes on the local network receive the packet and compare the destination IP with their own IP address. The node for which the IP address matches issues an ARP reply.

In our architecture, access routers will give the client nodes the illusion that the mesh network is a local broadcast network. For this end, each access router runs on its client access interface the *ARP Request Handler* module which is a modified ARP proxy. When a client node needs to communicate with a destination IP for which it has no IP to MAC mapping in its ARP cache, it broadcasts an ARP request.The access router's *ARP Request Handler* checks the LCL list in the *Client Management Module* to see if the destination is an associated client. If this is the case, the access router transmits the same ARP request on its access point interface. The communication between the two client nodes will be automatically bridged. If the destination is not a local associated node, the access router replies with an ARP reply message indicating that the access router's MAC address is associated with the destination IP address. By *faking* its identity, the access router accepts responsibility for routing packets to the *real* destination.

3.4 Routing Module

We extend Dynamic MANET On-Demand (DYMO)[2] [6] routing protocol to establish and maintain routes between communicating nodes in the mesh network. In the following we overview DYMO's operation, then we describe how access routers advertise their associated client nodes within routing messages and we end this section by explaining the DYMO extended operation for a mesh network.

DYMO overview: DYMO is a reactive adhoc routing protocol based on a RREQ/RREP route discovery. When a source node has data packets to send, it generates a *Route Request* (RREQ) message that floods throughout the wireless network. Upon receiving the RREQ the destination node sends in unicast a *Route Reply* (RREP) message to the source node. The propagation of the RREQ and RREP messages creates a bidirectional route between the source and the destination nodes. Once the route is set up, the source node starts delivering data packets. To detect the freshness of routing information and to guarantee a loop free operation, each node participating in DYMO maintains a sequence number. When a DYMO node generates a new routing message, it increments its own sequence number and inserts it in the routing message. Intermediate nodes compare the message sequence number with the node's last known sequence number to decide if received information is stale or not. Any of the wireless links can be lost at any time. This occurs when a node moves, crashes or is temporarily shut down, or due to the inherent variability of wireless links. Therefore, every node must monitor the link status with each of its neighbors to detect link breaks and invalidate the routing table entries which use those links. The most common strategy to accomplish this is by exchanging periodic HELLO messages.

Advertising client nodes: Client nodes see the network as a typical wireless LAN; routing on the mesh backbone is transparent for them. Since access routers provide network access to client nodes, they will be responsible for discovering routes on behalf of their associated clients. DYMO specification allows to append additional routing information to a routing message. We will exploit this option to allow access routers to advertise associated client nodes as these nodes don't have any routing capability. As clients are non DYMO nodes, they do not maintain sequence numbers to be used by the access routers when appending their addresses to routing messages. This implies that the access routers will either maintain a separate sequence number for each of their associated clients or use their own sequence number for the appended client node IP address. Both options are risky in practice. The freshness of routing information is identified by checking the value of the sequence number. A higher sequence number value means fresher information. DYMO nodes increment their sequence number value before issuing a new routing message allowing network nodes to detect

[2] DYMO is designed for flat topology adhoc networks. It cannot be directly applied in 2-tier Mesh networks.

valid from stale routing messages. This property cannot be satisfied when access routers maintain separate sequence numbers or use their own sequence numbers for client nodes. After a handover, a client may get a lower sequence number by its new access router.

To overcome this problem, we propose to use a new option that we call *Associated Node* to allow access routers to advertise their associated client nodes when required. The *Associated Node* option will be appended to DYMO routing messages. This option contains the IP address of the client node and a timestamp generated by the access router at the moment of building the routing message. The use of a timestamp allows to indicate the freshness of the client's related information. When a mesh node receives a routing message containing an *Associated Node* option, it treats the timestamp the same way it does with a sequence number. This means that mesh nodes maintain the association between the client IP address and the last received timestamp. When a mesh node receives a routing message with *Associated Node* option, it compares the received timestamp with its last known timestamp associated with the same client IP (if available) to decide whether the message is stale or not. Using timestamps for the *Associated Node* option relaxes the requirement of maintaining separate sequence number per client node. For this end, a synchronization mechanism should be implemented within the network. We use our synchronization mechanism described in [12] to synchronize the mesh nodes on the backbone level. This mechanism provides a synchronization accuracy in the order of few μsec in a multihop network. It is based on receiver to receiver synchronization to provide network wide synchronization with respect to one reference node in the network. Two mesh nodes receiving the same synchronization control message will compare the reception times to adjust their local clocks. Using this accurate time synchronization mechanism allows intermediate mesh nodes to detect the freshness of client's appended routing information by looking to the timestamp field. This remains true when client nodes move from one access router to another.

Extending DYMO operation: In this section we describe the modifications imported to DYMO to operate in the mesh environment. Mesh routers are responsible for discovering and maintaining routes on behalf of their communicating client nodes. To understand the extended routing operation, consider that client node C_1 associated with access router M_1 wants to communicate with destination client C_2 associated with access router M_2. When M_1 receives from C_1 a data packet destined to destination node C_2, it checks the RCL list of the *Client Management Module* to check for a match with the destination IP C_2. If no match exists, the routing module is contacted to discover a route to the destination IP C_2. The routing module then builds a Route Request message containing an *Associated Node* option. The route request message contains the following information[3]:

[3] DYMO uses the generalized packet format described in packetbb, however, for sake of simplicity we only show the information of interest contained in the routing messages.

Target Node : C_2 IP - C_2 sequence number[4]
Originator Node : M_1 IP - M_1 own Sequence number
Associated Node : C_1 IP - timestamp T_1

The message is flooded on the backbone level. When a mesh node receives the RREQ message, it updates its RCL list by adding that the client address C_1 associated with access router M_1; the routing table is also updated accordingly. Then the mesh node checks its LCL to see if the target node C_2 is an associated client. Only access router M_2 has a match; it issues a RREP message comporting an *Associated Node* option and containing the following information:

Target Node : C_1 IP - timestamp T_1 (from the RREQ)
Originator Node : M_2 IP - M_2 own Sequence number
Associated Node : C_2 IP - timestamp T_2

The RREQ and RREP messages allow mesh nodes on the path between M_1 and M_2 to update their RCL lists and their routing tables with the required entries. Now when M1 receives the RREP message it updates it's RCL list with an entry indicating that C_2 is associated with M_2.

3.5 Handoff and Mobility Support

The access point interfaces of the access routers form an extended basic service set (EBSS) allowing transparent client handover from one access router to another. Handover is initiated by the client node when it receives a stronger signal from a new access router. On the backbone level, routes toward client nodes must be updated following a client handover. DYMO routing protocol has the RERR functionality to announce that certain destinations are not available. When a mesh node receives a packet from another mesh router destined to a target node for which there is no available route, a RERR message is initiated. After issuing a RERR, a new route discovery procedure is required to build the new path between the communicating nodes.

This reactivity in the route re-establishment may not be suitable for time constrained applications. To limit the effect of route re-establishment delay, when an access router receives an event on its client management module indicating that a new client has just associated, it issues a Hello message including the *Associated Node* option to inform its neighbors that the new associated node is reachable through it. This message allows neighbor nodes and potentially the previous access router responsible for the newly associated node [5] (if the node has moved from one access router to another) to update their RCL tables and their routing entries.

[4] The last known sequence number of the target node if any.
[5] Generally, a client moves between neighboring access routers. If this is not the case, the route re-establishment will follow the RERR as described in DYMO specification.

3.6 Communication Handling

Communications involving client nodes in the mesh network can be classified into: communication between two clients associated with the same access router, communications between two clients associated with different access routers and communications between clients and the Internet.

Clients associated with the same access router: The client access interface of the access router bridges automatically packets between the two clients as they are attached to an access point. No further attention is needed here as the communication will not affect the mesh backbone.

Clients associated with different access routers: When a client node C1 associated with access router M1 wants to communicate with client node C2 associated with access router M2, the following setup takes place.

1. C1 broadcasts an ARP Request asking for the MAC address corresponding to C2's IP.
2. M1's ARP request handler replies with an ARP reply claiming that its MAC address is associated with IP C2.
3. C1 can start now sending data packets to C2. Upon receiving data packets from C1, M1 checks for a valid route toward C2. If a route exists no more processing is required. If no route exists go to step 4.
4. M1 generates a RREQ message including an *Associated Node* option to discover a route to destination node C2 and floods it within the network.
5. M2 receives the RREQ checks its LCL list for a match with the target node C2. If a match exists, M2 sends in unicast a RREP message including an *Associated Node* option.
6. M1 receives the RREP inserts an entry in its RCL indicating that C2 is associated with M2.
7. The route from C1 to C2 is set up. The data flow between the two nodes can flow now.

In addition to the previously listed steps, each access router updates its routing table whenever a change occurs in its RCL. For example, when receiving a RREQ or a RREP message including an *Associated Node* option.

Communication with the Internet: Communications from a client to an Internet destination follows the same rules as for two clients associated with different access routers except that the network's gateway is responsible for responding to RREQs for the destination node. Similarly, when the data traffic is from the internet to an internal client, the gateway will be responsible for discovering a route toward the client. In both cases, the gateway inserts as *Associated Node* option in the generated routing messages.

4 Conclusion and Ongoing Work

In this paper we presented the architecture of a reactive infrastructure based wireless mesh network. It is based on the DYMO/AODV routing protocol with a new extension, *Associated Node*, to advertise client nodes. We use timestamps to detect the freshness of clients' related routing information. We use an ARP request handler, an ARP proxy like module, to give the clients the illusion of a local network. DHCP is used to configure client nodes and to map between network and hardware addresses. Each access router maintains a list of its associated clients and the list of remote clients which are in active communications with its local clients. The work is ongoing to implement the proposed system on a real platform in the LOR department at Telecom SudParis in order to study its performance.

References

1. A. Agarwal and P. R. Kumar. Capacity bounds for ad hoc and hybrid wireless networks. *Computer Communication Review*, 34(3):71–81, 2004.
2. I. F. Akyildiz, X. Wang, and W. Wang. Wireless mesh networks: a survey. *Computer Networks*, 47(4):445–487, 2005.
3. Y. Amir, C. Danilov, M. Hilsdale, R. Musaloiu-Elefteri, and N. Rivera. Fast handoff for seamless wireless mesh networks. In *MobiSys*, pages 83–95, 2006.
4. J. Bicket, D. Aguayo, S. Biswas, and R. Morris. Architecture and evaluation of an unplanned 802.11b mesh network. *MobiCom 05*, pages 31–42, 2005.
5. S. Biswas and R. Morris. ExOR: Opportunistic multi-hop routing for wireless networks. In *SIGCOMM*, pages 133–144, 2005.
6. I. Chakers and C. Perkins. Dynamic manet on-demand (dymo) routing. *IETF Internet-Draft draft-ietf-manet-dymo-06 (work in progress)*, 'Oct. 2006.
7. S. Y. Cho, C. Adjih, and P. Jacquet. Association discovery protocol for hybrid wireless mesh networks. Rapport de Recherche Num: 5853, INRIA Rocquencourt, France, 'March 2006.
8. Y. Ge, L. Lamont, and L. Villasenor. Hierarchical OLSR : A scalable proactive routing protocol for heterogeneous ad hoc networks. In *WiMob 2005*, Canada, August 2005.
9. L. Iannone and S. Fdida. MeshDV: A distance vector mobility-tolerant routing protocol for wireless mesh networks. *IEEE ICPS Workshop on Multi-hop Ad hoc Networks: from theory to reality (REALMAN)*, 'July 2005.
10. P. Kyasanur and N. H. Vaidya. Routing and link-layer protocols for multi-channel multi-interface ad hoc wireless networks. *Mobile Computing and Communications Review*, 10(1):31–43, 2006.
11. D. C. Plummer. Ethernet address resolution protocol: Or converting network protocol addresses to 48.bit ethernet address for transmission on ethernet hardware. *IETF RFC 826*, 'Nov. 1982.
12. B. Wehbi, A. Laouiti, and A. R. Cavalli. Efficient time synchronization mechanism for wireless multi hop networks. *To appear in PIMRC 2008.*