

# An Association Discovery Protocol for Hybrid Wireless Mesh Networks<sup>1</sup>

Song Yean Cho      Cédric Adjih      Philippe Jacquet  
INRIA and Ecole Polytechnique  
France

Email: cho@lix.polytechnique.fr, Cedric.Adjih@inria.fr, Philippe.Jacquet@inria.fr

## Abstract—

Recently, various working groups of standardization bodies, have finalized or have been finalizing standards for wireless mesh networks (WMNs), which will provide some ad-hoc network capabilities to wireless networks. An example is the task group “S”, 802.11s, focusing on mesh extensions for Wi-Fi networks.

Such networks accommodate two kinds of nodes: *mesh routers* which form networks automatically in a similar fashion to ad-hoc networks ; and *mesh clients* which can simply associate with these mesh routers to access to the rest of the network. Because of the discrepancy of behavior between mesh routers and mesh clients, WMNs have a hybrid structure, where the mesh routers form a backbone, and where clients have no routing capability.

Routing in WMNs may be achieved with an extension of routing with two levels of information: traditional routing tables between mesh routers, complemented with *association tables* for linking mesh clients to mesh routers. For the first level, routing between mesh routers, can be used, for instance modified versions of MANET protocols. For the second level, we propose an Association Discovery Protocol (ADP): it allows each mesh router to determine where are located the other stations.

Our proposal had actually been integrated in the early 802.11s proposals [6], and in this article, our focus will be on such 802.11 mesh networks.

Because the ADP has parameters which can be tuned, a performance analysis of the protocol is essential. In this article, we describe this protocol, and provide a analytic model of its performance. The performance evaluation is confirmed by simulation results.

## I. INTRODUCTION

Wireless Mesh Networks (WMNs) have been proposed as a prominent network solution for ubiquitous networks [1], and industry standard groups such as IEEE 802.11 [2][3][4], 802.15[7] and 802.16[8] are developing new specifications for WMNs. The recent

<sup>1</sup>This work was partly funded by Samsung Electronics Co, LTD. Part of this work was realized while Song Yean Cho was at Samsung Electronics. Song Yean Cho, Cédric Adjih and Philippe Jacquet are currently with the Hipercom Team, of INRIA Rocquencourt and École Polytechnique.

broad interest about WMNs is due to two major features of WMNs. First, WMNs are capitalizing on the self-organising aspects of ad-hoc networks, and the ease of deployment with minimal preparation, requiring less administration and maintenance. Second, WMNs (particularly, for 802.11 networks) can capitalize on a broad installed base, and on a technology which has been already developed: they enable mesh clients to access networks, without requiring them to execute an additional routing protocol (for instance, 802.11 stations). Instead of running a complex routing protocol, clients simply associate themselves with mesh routers and rely on mesh routers to access the whole WMNs: the routing on the wireless mesh routers is transparent for the client. This feature may also be used by design, in order to isolate the routing functionality from the clients: then different deployment of WMNs with different features, could still accommodate the same wireless mesh client. This also allows lighter clients and simpler participation in heterogeneous networks.

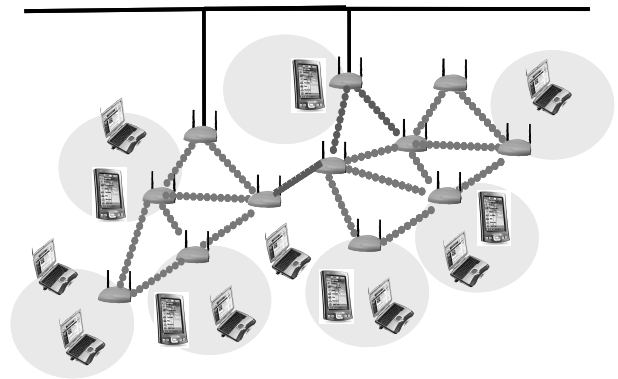


Fig. 1. Architecture of hybrid wireless mesh networks

The figure 1 illustrates two main components of WMNs: the *mesh routers* and *mesh clients*. Mesh routers create multihop networks, that are self-configuring and

self-healing, by executing routing protocols. The routing protocols for WMNs need not to be much different from those of wireless ad hoc network in general and Mobile Ad hoc NETWORK (MANET) [20] in particular. For MANET, several routing protocols such as OLSR (Optimized Link State Routing Protocol) [9], AODV (Ad hoc On demand Distance Vector) [12], TBRPF (Topology Broadcast based on Reverse-Path Forwarding) [14] and DSR (Dynamic Source Routing)[13] have been proposed, and some variants of such protocols are being used for WMNs.

Unlike mesh routers, mesh clients should associate with mesh routers to access networks. To associate with mesh routers, mesh clients use specific attachment protocols such as page/inquiry for Bluetooth or *association request/reply* for IEEE 802.11.

Obviously, in order to accommodate the mesh clients participating in a WMN, the mesh routers should perform new operations in addition to the functioning of the classical ad-hoc network routers. The basic MANET routing protocols [9], [12], [14], [13] are indeed operating on flat topology; hence it is insufficient to find paths between mesh clients of the hybrid network. In order to collect complementary information, mesh routers can execute an additional auxiliary protocol.

In this article, we propose such a solution: an association discovery protocol for mesh networks. Using this protocol, mesh routers can compute routes to the mesh clients associated to other mesh routers (by means of an association table). Our protocol is simple and general; it can be used to complement any ad-hoc network routing protocol. However it targets more specifically 802.11s, for which it was initially developed. Additionally, because it is proactive in nature, it is more naturally suited to run with the optional 802.11s OLSR variant, Radio-Aware OLSR (*RA-OLSR*), integrated in 802.11s [6].

This article is organized as follows. First, we review some related work. Then, we briefly explain how the OLSR routing protocol can operate to compute routing tables (for all mesh routers), and then we describe the proposed ADP working in conjunction with OLSR. Afterwards, we estimate the performance of the ADP through an analytical model and evaluate our estimation through simulations. After presenting and analyzing simulation results, we present our conclusions.

## II. RELATED WORK

A hybrid network structure is not a unique feature of WMNs. Hybrid routing protocols such as FSR [15], ZRP [16] or CBRP [17], Landmark (Landmark+OLSR [18]) have been explored for MANETs with some hybrid structures. But their hybrid structure is in general different from that of WMNs in two aspects: WMNs admit the

presence of non-router nodes and can use a flat address space.

Assuming the existence of a routing protocol, between mesh routers, the problem that we are trying to solve is straightforward: *how to exchange information indicating which station (mesh client) is attached to with mesh router ?*

Routing protocols themselves integrate some functionalities to inject some external routes in the network. For instance, OSPF has its own mechanisms to import non-OSPF routes with specific types of OSPF LSA messages [10], [11]. These messages are used to exchange routes that are external to the OSPF network, and are then used to complement the routes computed by OSPF.

Similarly, in order to integrate nodes without routing functions, OLSR also provides a mechanism called *Host and Network Association (HNA)* to exchange information about routes to non-OLSR nodes. However, in the current specification [9], HNA in [9] is not well adapted to non-OLSR nodes for which the last hop (an OLSR node) may be changing quickly: an OLSR node periodically distributes HNA messages listing all its non-OLSR nodes. There are two problems, the first one is the necessity of performing a full diffusion of the HNA-database when a node disappears, and the second is related, it is the large overhead of such messages, when the number of associated stations is large. An approach the mixed layer 2/layer 3 approaches improving on HNA messages [23].

Looking at a broader picture, more general protocols also exist to diffuse distributed sets of information, such as OSPF-style database exchange for OLSR [21], Gossip-based approaches [22] and on-demand request/response for reactive protocols. Unlike these protocols, our protocol is specifically designed to address the following information exchange problems:

- Information items (which mesh client is associated to which mesh router) with sequence numbers
- Medium-sized information set (potentially too large to be diffused periodically, but for which a single level of hierarchy is sufficient)

The main feature of ADP proposed is to limit the overhead of repeating information which is already widely known. Using the ADP in conjunction with OLSR, adds another benefit: OLSR has an optimized flooding mechanism (MPR-flooding) which can be and is used. In the next section, we explain OLSR briefly.

## III. OLSR ROUTING PROTOCOL

The OLSR routing protocol, which can be used to select paths in WMNs, is a proactive link-state routing protocol, employing periodic message exchanges to update topological information in each mesh router. Because OLSR is specifically designed to operate in the

context of wireless multi-hop networks such as MANET, it provides an optimized flooding mechanism, called MultiPoint Relay (MPR)-flooding, used to diffuse topology information. MPR flooding optimizes flooding by minimizing the redundant retransmissions of Topology Control (TC) messages. Minimization is achieved by limiting the forwarders of messages to some MPRs. A set of MPRs relays is a small set of neighbors through which a sender can reach all two hop neighbors.

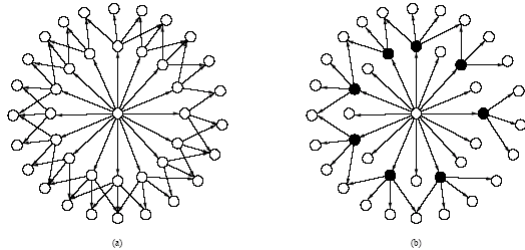


Fig. 2. Pure flooding vs. MPR flooding

As figure 2 shows, messages can be broadcast from the source to the entire WMNs through MPRs' relaying. The first figure in figure 2 shows the retransmission of pure flooding, where every node retransmits the packet and the second figure shows the retransmission of MPR flooding, where only MPR nodes retransmit the packet. Only with MPRs' retransmission, the source can broadcast successfully the packet to every node in networks. In addition, a node can reach any node in network only utilizing links between MPRs. Thus setting up the paths may not require all links between mesh routers. Information about links with MPRs is sufficient, by property of the MPR (and because all nodes have selected an MPR set). Thus mesh routers can simply transmit the addresses of all their MPR selectors with their address in TC messages. Even if the topology information obtained from received TC messages is a partial topology of whole WMN, the shortest path obtained from this partial topology has the same length as the shortest path from the full topology [19].

For the specific application of 802.11s Mesh Networks, a variant of OLSR is used as an option: *Radio-Aware OLSR*. It integrates essential features for selecting links with good quality.

Now, considering the hybrid structure of WMNs, the association between mesh clients and mesh routers must be discovered in order to complement the topology information of the mesh routers.

#### IV. ASSOCIATION DISCOVERY PROTOCOL

The Association Discovery Protocol, which is the main topic of this article, can be used to complement any

of routing protocol, as previously indicated. However we had designed it specifically with 802.11s Mesh Networks in mind: "802.11s" is the the task group 'S' of the 802.11 working group, in charge of proposing mesh networks extensions to 802.11. Indeed, our protocol had been integrated in the early drafts of 802.11s in [6] ("*Associated Station Discovery*").

Such mesh networks distinguish two types of nodes<sup>1</sup>:

- Mesh routers, running the routing protocol, and able to associate mesh clients.
- Mesh clients (legacy 802.11 STA), which *associate* themselves to a mesh router.

The base mechanism of ADP is the following: mesh routers diffuse the whole set of mesh clients associated to themselves. It is hence a proactive protocol, similar in spirit to the functioning of OLSR: in both cases the topology (associated station) information messages must be refreshed within a guaranteed interval (i.e. before the expiration). However, in addition to periodic message exchange, in case of topology/association change, faster updates are possible, and are desirable, in optimized implementations.

As explained in section I, mesh clients rely on mesh routers to compute paths to their destination, and this computation requires both routing tables and association tables. To obtain the two types of database (tables), mesh routers exchange the list of mesh clients associated with themselves in addition with the traditional information from the routing protocol ; they store and maintain the received information using two information bases:

- *Local Association Base (LAB)*: Each mesh router keeps track of mesh clients associated with itself. This information base is updated whenever associated mesh clients leave or new mesh clients join.
- *Global Association Base (GAB)*: Each mesh router maintains a GAB to record which station is associated to which mesh router in the entire WMN. Upon receiving LAB from all other mesh routers, the GAB is updated. Hence the GAB contains the union of all the LAB, of each mesh router in the WMN.

The full set of messages for information exchange used by the protocol is in section ??.

To fill the GAB of other routers, each mesh router broadcasts its full LAB periodically. These additional periodical messages generate overhead. This feature brings an interesting trade-off between bandwidth use and reactivity to changes. Considering that a LAB is not modified when there is no new association or disassociation, an

<sup>1</sup>*Mesh Points*, which are clients able to run the routing protocol are also possible in 802.11s, but for our description, they are identical to mesh routers without clients

optimization is possible: diffusing only updates (newly associated, or disassociated stations).

There is, however, a fundamental issue with the exchange of *differential* updates: message loss. When a differential update is lost, it is not sufficient to detect the loss of the message and have it repeated: because additional changes could occur (including re-association of disassociated stations for instance) before the message repeating, it is complex to provide recovery after message loss, using uniquely differential updates, without maintaining a time-ordered log of all changes. Hence, an additional mechanism to check information base *consistency*, and a mechanism to exchange full (non-differential) updates has to be integrated.

A main feature of our protocol, is to restrict itself to the two last mechanisms, while offering performance comparable to differential updates. To do so, every mesh router with a large number of mesh clients, can divide its LAB into several smaller *blocks*. Then updates of association/disassociation of one or few stations, are made by diffusion of the one or the few small blocks containing those addresses. Since in 802.11 type of networks, the MAC overhead is important for small packets, the cost of either sending one address or sending a few addresses in the same message is expected to be on the same order of magnitude.

#### A. General Protocol Operation

Precisely, the protocol operates with three kinds of messages, detailed in section ??:

- LABA messages: used for diffusion of the *full* content of one, part of, or all blocks of the LAB of the originator node.
- LABCA messages: used for diffusion of *checksum* of one, part or all blocks of the LAB of the originator node. The purpose of such messages is to avoid repetition of already widely disseminated information: a checksum of the block is diffused instead of the block itself.
- ABBR messages: used to require a set of blocks, typically upon receiving a mismatching LABCA checksum for some block(s), symptom of message loss.

Notice the inherent tradeoff on block size: larger blocks imply larger LABA messages, and while small blocks imply larger LABCA messages.

With this set of three messages, a large number of protocol variants could be implemented, depending on client mobility, packet loss, and communication patterns. Generally, blocks, messages intervals, may all be adjusted dynamically, and need not to be identical for all blocks. In addition, all messages need not to be sent by/to the mesh router originally holding LAB

information, although in this last case this would need to be predetermined for interpretability. And LAB updates may be sent preferably to some mesh routers more critical.

Note also that instead of a checksum, a simple sequence number per block could alternatively be used, matching the methods of OSPF for instance. The advantage of the checksum is that it allows to arbitrarily change the repartition of the addresses into blocks, a feature which is not currently used.

In the following, we will focus on a simple variant of the protocol described in section IV-B.

#### B. Simple Protocol Operation

In this section, we are describing a simple protocol operation, which still uses the ability to decrease the ADP overhead using checksums.

In this protocol operation, there are two operating modes: *full* mode and *checksum* mode. Initially mesh routers operate in full mode. After a given duration, mesh routers which did not sense any change in their LAB, will start to operate in checksum mode. Any change in their LAB resets mesh routers back to operate in full mode.

1) *Full Mode*: In full mode, mesh routers periodically broadcast the whole contents of their LAB (all blocks).

2) *Checksum Mode*: If the network becomes stable and few mesh clients are moving, the LAB of mesh routers will not change much. In this case, mesh routers avoid generating heavy overhead by simply diffusing checksums representing the status of their LAB rather than sending the all their content, in LABCA messages.

Upon receiving these checksums, a receiving mesh router cannot populate entries in its GAB, but it can verify them. If a checksum mismatch is found, this implies that the mesh router has missed some updates of the LAB of the mesh router which originated the message. In this case, the mesh router will send a request (ABBR) for the mismatching parts to originator mesh router in order to restore the consistency of its GAB by recovering the lost information. Upon receiving these requests, the mesh router switches to full mode, thus emitting the contents of its whole LAB.

## V. ANALYTICAL MODEL

As described in previous section, the mesh routers executing the ADP are switching between two operation modes; depending to the stability of the associated mesh clients.

Messages are emitted periodically ; after a fixed number of LABA emission intervals without message loss (i.e. without ABBR requests) and without changes in station association (i.e. change in the LAB), the mesh

routers switch to checksum mode. The fixed number of LABA emission intervals is a parameter of each mesh router of the system. In order to evaluate the performance of the system, the following two metrics are used: *Packet Error Rate (PER)* (i.e. amount of packets lost due to obsolete routing information) and the control overhead. In this section, we are providing an analytical model of the performance for this protocol.

### A. Packet Error Rate (PER)

In our model, mesh clients move independently and their movements are not synchronized. To focus on PERs' change according to the ADP's operations, data packets are assumed to be lost only when mesh clients move from the sojourned mesh router and notifications of this movement are lost. The loss time when the position of mesh clients is not known is shorter than the sojourn time when mesh clients associate with the mesh router.

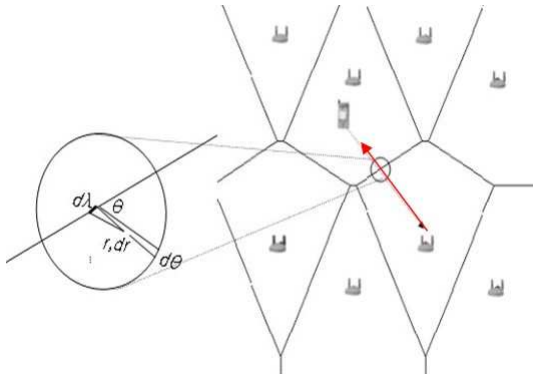


Fig. 3. The change of association with mesh clients' mobility

Under this assumption, mesh router  $i$  changes its operation mode from full mode to checksum mode when its LAB does not change for  $h_i \times t_i$ , where  $h_i$  is mesh router  $i$ 's control message distribution interval and  $t_i$  is the number of message intervals for mesh router  $i$  to switch from full to checksum mode. As mesh clients move, they associate with each mesh router several times for some duration. We call *life time* ( $L_i^\alpha$ ) the duration when a mesh client  $\alpha$  associates with a mesh router  $i$ , and we call *frequency* ( $\tau_i^\alpha$ ) the number of times that one mesh client  $\alpha$  sojourns with mesh router  $i$ . Packets are lost as long as the control message is not received (*the control information loss duration*). PER between mesh clients can be derived from the *average control information loss duration (ACILD)* between mesh routers. One the ACILD is known, considering all cases where a mesh client  $\alpha$  can be located and utilizing the fact that a mesh client  $\beta$  stays for an average time  $L_j^\beta$ , the PER from mesh client  $\alpha$  to mesh client  $\beta$  is:

$$\sum_{(i,j), i \neq j} \tau_i^\alpha L_i^\alpha ACILD_{ij} \tau_j^\beta \quad (1)$$

In addition, because mesh clients move with a random walk in our model,  $\tau_i^\alpha$  and  $L_i^\alpha$  depend on the area that mesh routers cover. More precisely,  $\tau_i^\alpha L_i^\alpha$  is equal to  $\frac{A_i}{A}$ , where the total network area is  $A$  and mesh router  $i$  covers an area  $A_i$ . Similarly, as mesh router  $i$  has longer border, the probability that mesh client  $\alpha$  crosses the border becomes higher, and the frequency with which mesh client  $\alpha$  sojourns with mesh router  $i$  ( $\tau_i^\alpha$ ) also increases. Precisely,  $\tau_i^\alpha$  is proportional to  $B_i$ , the border of the area  $A_i$  covered by mesh router  $i$ . When the mesh client  $\alpha$  moves at speed  $v^\alpha$ , the probability that it crosses the border on the portion  $d\lambda$  during time interval  $(t, t + d\lambda)$  is:

$$\frac{d\lambda \sin\theta}{2\pi A r} r dr \quad (2)$$

We can derive 2 from the mesh router's area as seen in figure 3. At time  $t$ , the mesh client  $\alpha$  must be in the half of the disk of radius  $v^\alpha dt$  and moves toward the portion  $d\lambda$  as seen in figure 3. Considering the mesh client  $\alpha$  at a distance between  $r$  and  $r + dr$  in the cone at angle  $\theta$ , the probability that the mesh client  $\alpha$  is within this area is  $\frac{r dr d\theta}{A}$ . When the angle at which mesh client  $\alpha$  sees the portion  $d\lambda$  is  $\frac{d\lambda \sin\theta}{r}$  and the speed of mesh client  $\alpha$  toward this direction is  $\frac{d\lambda \sin\theta}{2\pi r}$ . Therefore the probability that the mesh client  $\alpha$  crosses the border on the portion  $d\lambda$  during the time  $dt$  is:

$$\int_0^\pi d\theta \int_0^{vdt} \frac{d\lambda \sin\theta}{2\pi A r} r dr = \frac{v^\alpha d\lambda}{\pi A} \quad (3)$$

On the total border length  $B_i$ , the probability that the mesh client  $\alpha$  crosses  $B_i$  becomes  $\frac{v^\alpha \times B_i}{\pi A}$ . Consequently, packet error rate between the mesh client  $\alpha$  and  $\beta$ ,  $PER_{\alpha\beta}$  is equal to

$$\sum_{(i,j), i \neq j} \frac{v^\alpha \times B_i}{\pi A} L_i^\alpha \times ACILD \times \frac{v^\beta \times B_j}{\pi A} \quad (4)$$

To compute the PER using 4, we need the ACILD and it can be derived from  $r_{ij}$ , the probability to lose control messages between mesh route  $i$  and mesh route  $j$ . When a mesh router does not operate the ADP, it always run in full mode, and then ACILD is

$$h_i \sum_{k=0}^{infy} k r^k (1-r) = \frac{h_i}{1-r_{ij}} \quad (5)$$

Unlike for equation 5, mesh routers may switch between operation modes, and we have to consider control information loss duration for both modes. Mesh router  $i$  fails to switch its operating mode to checksum when it does not receive any control message for  $h_i$  intervals. Thus, the probability that mesh router  $i$  fails to switch its operation mode to checksum for duration  $h_i$  is  $r_{ij}^{h_i}$ , and the probability that mesh router  $i$  succeeds it is

$1 - r_{ij}^{h_i}$ . Accordingly, when mesh router  $i$  fails to switch to checksum mode, its control loss duration is:

$$t_i + \frac{1}{1 - r_{ij}} \quad (6)$$

In addition, when mesh router  $i$  can switch to checksum mode, its control information loss duration ( $CILD_{succeed}$ ) becomes:

$$\frac{t_{ij}}{1 - r_{ij}} \times \sum_{k=0}^{h_i-1} k r_{ij}^k (1 - r_{ij}) = \frac{1 - r_{ij}^{h_i}}{1 - r_{ij}} - h_i r_{ij} \quad (7)$$

Because mesh routers running the ADP must consider loss duration both ways, average control loss duration (ACILD) is:

$$(1 - r_{ij}^{h_i} \times (eq (6))) + r_{ij}^{h_i} \times ((eq (7)) + ACILD). \quad (8)$$

Reducing 8, ACILD is  $\frac{r_{ij}^{h_i}}{1 - r_{ij}^{h_i}} (t_i + \frac{1}{1 - r_{ij}}) + \frac{1 - r_{ij}^{h_i}}{1 - r_{ij}} - h_i r_{ij}$

Finally, difference of control loss interval between mesh router with the ADP and without ADP becomes  $h_j \frac{r^t}{(1 - r^t)(1 - r)}$  and difference of PERs between mesh router with ADP and without ADP becomes

$$\sum_{(i,j) \neq j} \frac{v^\alpha \times B_i}{\pi A} L_i^\alpha \times h_j \frac{r^t}{(1 - r^t)(1 - r)} \times \frac{v^\beta \times B_i}{\pi A} \quad (9)$$

To optimize the ADP, mesh routers choose  $t_i$  minimizing expression 9 under given conditions.

## B. Control Overhead

When mesh router  $i$  operates in full mode, the size of the control messages for distributing its LAB is proportional to the average number of mesh clients associated with mesh router  $i$ . In contrast, the overhead in checksum mode does not change regardless of the number of clients assuming the number of blocks is fixed. If the ADP represents each mesh client in  $C_1$  bytes and the hash function generate checksum output as  $C_2$  bytes where  $P_{checksum}^i$  is the probability that mesh router operates in checksum mode, the decreased overhead per  $h_i$  by introducing checksum mode is

$$C_1 M_i - C_1 P_{full}^i M_i + C_2 P_{checksum}^i = P_{checksum}^i (C_1 M_i - C_2) \quad (10)$$

As expression 10 shows, the overhead for mesh router starts to decrease if  $M_i$  is greater than  $\frac{C_2}{C_1}$ . If  $C_1 = C_2$ , the control overhead decreases if the mesh clients just outnumber the mesh routers. This overhead decrease is also related to the mesh client's mobility,  $L_i^\alpha$  and  $\tau_j^\alpha$ . As mesh client  $\alpha$  sojourns with mesh router  $i$  for  $L_i^\alpha$  with  $\tau_j^\alpha$  frequency, the average number of mesh clients associated with mesh router  $i$  ( $M_i$ ) equals  $\sum_\alpha \tau_j^\alpha L_j^\alpha$ . Combining this with eq. 10, the overhead decrease is:

$$P_{checksum}^i (C_1 \sum_\alpha \tau_j^\alpha L_j^\alpha - C_2) \quad (11)$$

To use eq. 11 we should find the  $P_{checksum}^i$ , the probability that the mesh routers are in checksum mode.  $P_{checksum}^i$  depends on when mesh routers change their operation mode from full to checksum. This is when their LABs did not change for  $h_i \times t_i$ . It means that the possibility changes according to mesh client's mobility, i.e., life time ( $L_i^\alpha$ ) and frequency ( $\tau_i^\alpha$ ). If mesh clients move from the area of one mesh router to the area of another mesh router with Poisson distribution, the possibility that the LAB of mesh router  $i$  does not change for ( $h_i$ ) is:

$$e^{-(2 \frac{M_i}{L_i}) h_i} \quad (12)$$

In equation 12,  $M_i$  is the number of mesh clients associated with mesh router  $i$ .  $M_i$  is related with the mobility of mesh clients and their number. More precisely,  $M_i$  is  $N \times \tau_i L_i$ , where  $N$  is the total number of mesh clients. Similarly to  $\tau_i^\alpha$  and  $L_i^\alpha$ ,  $\tau_i$  is the sum of the frequency with which mesh clients associated with mesh router  $i$ , and  $L_i$  is the sum of sojourn time of all mesh clients with mesh router  $i$ . As a result, the probability that the mesh router  $i$  operates in checksum mode  $P_{checksum}^i$  is:

$$e^{-(2N \times \tau_i \times h_i) \times t_i} \quad (13)$$

Finally, we can choose  $t_i$  to adjust the control overhead decrease using the following equation:

$$e^{-(2N \times \tau_i \times h_i) \times t_i} (C_1 \sum_\alpha \tau_j^\alpha L_j^\alpha - C_2) \quad (14)$$

## VI. SIMULATION

To evaluate our analytical model and the ADP itself, we performed simulations using grid topologies as shown on figure 4.

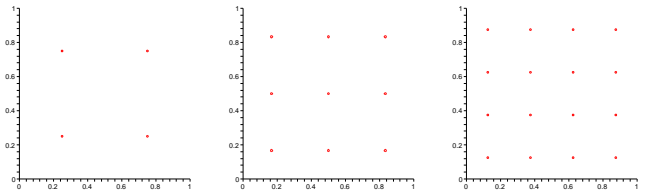


Fig. 4. Mesh routers in grid topology

We compared the PER and control overhead, in two sets of simulations: the first ones with only full mode, the second with both full and checksum modes. Simulations were ran with the parameters given in table I, (except for switching interval). To remove other factors affecting PER and control overhead, a Null MAC was used (no collision, infinite speed). The mobility is the maximum distance where one 802.11 legacy station moves one time and is proportional to the transmission range.

TABLE I

SIMULATION AND SCENARIO PARAMETERS

Simulation Parameters	
Control msg loss rate per link	0.1
Mobile station num	3 x Mesh AP num
Control message interval	2 sec
Transmission range between Mesh routers	0.53(2x2), 0.35(3x3), 0.26(4x4)
Scenario Parameters	
802.11 legacy stations speed	0.01,0.03,0.05 x TR
Simulation time	20000 sec
Mobility model	Random walk
Pause time	5 sec
Traffic pattern	constant bit rate, 512 bps
max connection	0.1 x mesh client num

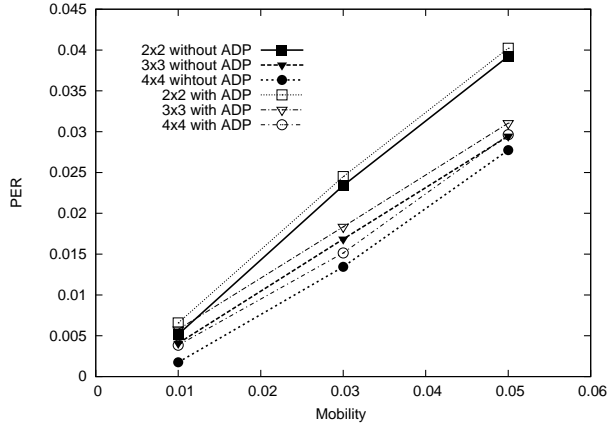


Fig. 5. Comparison of PERs with and without ADP optimization

If mesh routers do not use the ADP, they always distribute the whole LAB. Though distributing the whole LAB can improve PER, it consumes considerable bandwidth. To measure the amount of PER decrease by operating the ADP, we compare PERs from a mesh router with both checksum and full modes with PERs from a mesh router distributing the whole LAB. Figure 5 shows PERs from these two kinds of mesh routers. The PERs from a mesh router using ADP is slightly lower than other, but their difference is just less than 0.002. This small improvement shows that ADP allows the mesh router to maintain its PERs at the same level as when it distributes the full LAB periodically.

While keeping its performance as described above, ADP decreases the control overhead as shown in figure 6 after adjusting control message distribution interval  $h_i$ . If a mesh client moves slower than 0.05 x transmission range per a second, for example at 0.003 x transmission range, the control overhead decreases from 8 to 2 bytes per control message distribution interval  $h_i$ . The fact that the mesh router can decrease the control overhead using ADP supports the fact that ADP saves bandwidth by optimizing the control messages to distribute mesh routers' LAB.

In figure 6, control overhead decreases to almost zero with 0.05 mobility in grid 4x4. This overhead fall is due to the dramatic decrease in the possibility that

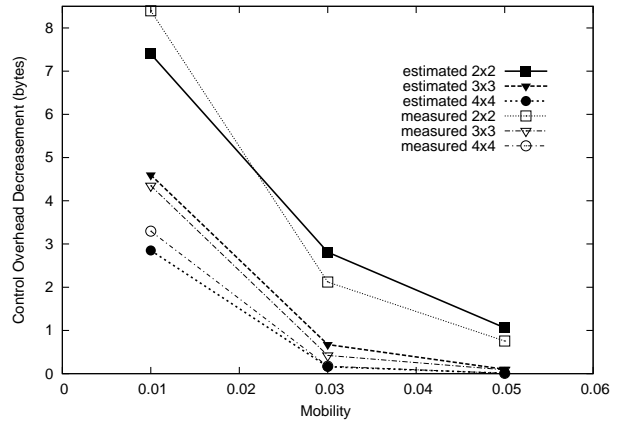


Fig. 6. Control overhead decrease

mesh router  $i$  operates in checksum mode. As analyzed by our model, a mesh client speed faster than 0.05 x transmission range per second negates the possibility for a mesh router to operate in checksum mode and to decrease the control overhead by utilizing ADP. This result demonstrates the accuracy of the estimation made by our model on the control overhead. Simulation results in figure 6 also confirm this. Moreover, the control overhead decrease also shows that ADP saves bandwidth by optimizing control message to distribute LAB.

## VII. CONCLUSION

In the architecture that we have proposed, the mesh routers are running not only a routing protocol to calculate their routing table but also an Association Discovery Protocol, whose task is to distribute the list of mesh clients associated with them. This Association Discovery Protocol had been integrated in an early draft of 802.11s specifications. We have described its principles, and some design decisions.

One of the challenge is to decrease the additional control messages overhead. This additional control overhead might not be ignored because a mesh router may associate with a large number of mesh clients, and in the proactive operation that was proposed, the mesh routers should know the entire lists of mesh clients associated with other mesh routers. Thus the mesh router should (periodically) distribute information about all mesh clients associated with them. In this case, the additional overhead to distribute information may well become larger than the overhead from the wireless mesh routing protocol. To answer this challenge, the proposed ADP divides association information into blocks, and can switch between two operating modes (per block): when part of its LAB is stable, a mesh router may issue only checksums to represent the content of its LAB, and refresh it for other routes (checksum mode). Otherwise,

it can still transmit full block information (full mode). A version of the protocol was analyzed, where the switch between full and checksum mode is made for the entire set of blocks.

As the analytical model and simulation results demonstrate, this capability of transmitting checksums is reducing the additional control overhead of ADP while keeping LABs consistent in the entire WMNs. More generally, the ADP proposed could be adapted to a wide variety of hybrid wireless networks.

## REFERENCES

- [1] Akyildi, I.F., Wang, X., and Wang, W., "Wireless Mesh Networks: A Survey," Computer Network Journal (Elsevier), Vol.47, pp.65-80, March 2005.
- [2] IEEE Std 802.11-1999 (Reaff 2003) "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".
- [3] "Terms and Definitions for 802.11s" IEEE 802.11-04/1477r4, document of the 802.11s working group.
- [4] "Functional Requirements and Scope for 802.11s" IEEE 802.11-04/1174r13, document of the 802.11s working group.
- [5] "Scalable Station Association Information Handling" IEEE 802.11-06/1842r3, documents of the 802.11s working group
- [6] "IEEE 802.11 TGs draft 0.03" IEEE 802.11 Task Group 3 Draft 0.03 documents of the 802.11s working group, August 2006.
- [7] P. Kinney, "IEEE 802.15 General Interest in Mesh Networking" IEEE 802.15 Request for Information of a Mesh Network Study Group, presentation slides, November 2003.
- [8] P.Piggin, B.Lewis, and P. Whitehead "Mesh Networks in fixed broadband wireless access: multipoint enhancements for the 802.16 standard" IEEE 802.16 presentation slides, July 2003.
- [9] T. Clausen and P. Jacquet (ed.), "Optimized Link State Routing Protocol (OLSR)," IETF RFC 3626, October 2003.
- [10] J. Moy (ed.), "Open Shortest Path First Routing Protocol (OSPF) Version 2," IETF RFC 2328, April 1998.
- [11] J. Moy, "OSPF anatomy of an internet Routing Protocol," Addison-Wesley, January 1998.
- [12] C.Perkins, E. Royer and S.Das, "Ad hoc On-demand Distance Vector Routing (AODV)," IETF RFC 3561, July 2003
- [13] D. Johnson, D. Maltz, Yih-Chun Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)", draft-ietf-manet-dsr-10.txt, July 2004 (work in progress).
- [14] R. Ogier, F. Templin, M. Lewis, "Ad hoc On-demand Distance Vector Routing (AODV)", IETF RFC 3684, February 2004.
- [15] M. Gerla, G. Pei, X. Hong and T. Chen, "Fisheye State Routing Protocol (FSR) for Ad Hoc Networks," Internet Draft, June 2001.
- [16] Z. J. Haas, M. Perman and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft, July 2002 (work in progress).
- [17] M. Jiang, J. LI, and Y. C. Tay, "Cluster Based Routing Protocol (CBRP)", Internet Draft, June 1999 (work in progress).
- [18] Mario Gerla, Xiaoyan Hong, Kaixin Xu, Zhihan Lu, Charmaine Flores, "LANMAR + OLSR: A Scalable, Group Oriented Extension of OLSR", OLSR Interop and Workshop, August 6-7th 2004, San Diego.
- [19] Philippe Jacquet, Pascale Minet, Paul Muhlethaler, and Nicolas Rivierre. "Increasing reliability in cable-free radio lans: Low level forwarding in hiperlan.", Wireless Personal Communications, 4(1):65-80, January 1997.
- [20] "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", IETF RFC 2501, 1999.

- [21] T. Clausen, P. Jacquet and E. Baccelli, "OSPF-style Database Exchange and Reliable Synchronization in the OLSR", INRIA Research Report RR-5283, July 2004.
- [22] Zygmunt J. Haas, Joseph Y. Halpern and Li Li, "Gossip-Based Ad Hoc Routing", Infocom 2002.
- [23] H. Okada, K Mase, M.Nozaki and B. Zhang, "Low-Overhead and Low-Processing Strategy of STA Association Information for RA-OLSR in IEEE802.11s", IEICE, March 2007.