Efficient Multicast Routing in Wireless Mesh Networks Connected to Internet

Pedro M. Ruiz and Francisco J. Galera
Fac. Informatica, Campus de Espinardo, E-30100
Espinardo, Murcia, Spain
{pedrom, fran}@dif.um.es

Christophe Jelger
Fraunhofer FOKUS,
Berlin, Germany
cje@fokus.fraunhofer.de

Thomas Noel
Louis Pasteur University,
Strasbourg, France
noel@dpt-info.u-strasbg.fr

***Abstract*— Wireless Mesh Networks (WMNs) have emerged as one of the new hot topics in wireless communications. They consist of a number of static wireless routers which form an access network for end users to IP-based services. Unlike traditional WLAN deployments, wireless mesh networks provide multihop routing, facilitating an easy and cost-effective deployment. In this paper, we focus in the provision of efficient multicast routing on such wireless mesh networks, and its seamless interconnection to wired IP multicast services. The proposed architecture and protocols allow for a ready deployment without changes on the existing networking equipments in the fixed network or in end user's devices. Our simulations and empirical evaluation on a real wireless mesh network demonstrate that the proposed approach offers a good performance and its highly scalable.**

I. Introduction and Motivation

Multicast is a key technology for future wireless networks. It provides efficient communications among a group of nodes, and helps at reducing the bandwidth consumption of many applications and services such as service discovery, videoconferencing, distributed gaming, etc. This is specially appropriate in wireless environments where bandwidth is scarce and many users are sharing the same wireless channels. In particular, for WMNs, multicast can represent a huge enhancement of the network capacity by taking advantage of links which can be shared by multiple users to receive the same data, which is transmitted only once.

During the last few years, some work has been done concerning the integration of mobile ad hoc networks and the Internet. In such scenarios, commonly known as *hybrid* ad hoc networks, one or multiple nodes are attached to the Internet and act as Internet gateways for the other nodes of the MANET. Wireless mesh networks follow a similar principle of operation, but unlike MANETs, the core of the network is assumed to be static. End-users are free to move and change their point of attachment to the mesh network at any time. Thus, most of the schemes for hybrid MANETs can also be used for WMNs. Unlike most of the previous works on hybrid MANETs in the literature, we focus on the particular issues associated to integrated multicast scenarios.

Being connected to the Internet has strong implications on the addressing scheme of a WMN. In private WMNs without Internet connectivity the addressing scheme can be flat in the sense that all nodes do not necessarily need to belong to the same logical IP subnet. However, when the WMN is connected to the Internet, nodes are required to have a topologically correct and globally routable IP address, if one wants to avoid the use of network address translation (NAT). Needless to say that for the particular case of providing multicast routing in those hybrid MANETs, the implications of address management are even stronger. The reason being that standardized multicast routing protocols used in fixed IP networks rely on the assumption of topologically correct IP addresses. For instance, multicast access routers usually perform a process called *RPF-check* on every incoming packet. This process drops any packet which arrives at an interface which that router would not use to reach the source of the packet. Thus, address auto-configuration is one of the key elements for a fully-integrated and seamless multicast interworking for WMNs connected to Internet.

Unfortunately, classical mechanisms for address auto-configuration in traditional IP networks are not feasible for ad hoc networks because of their multi-hop nature. The same happens with traditional multicast functions such as group membership. Topological changes and the presence of multiple gateways are key issues that need to be addressed. The mechanism used for address auto-configuration should allow ad hoc nodes to discover routes towards the gateways. Therefore, address auto-configuration and gateway discovery mechanisms must interoperate with the routing protocols used within the WMN.

In this paper, we propose an integrated solution for efficient multicast routing in WMNs. The proposed scheme consists of an efficient tree construction scheme which manages to reduce data overhead compared to traditional ad hoc routing protocols. To do that, it takes fully advantage of the broadcast nature of the wireless medium. We also extend that routing protocol with group membership functionalities compatible with those currently used in the Internet, allowing for the ready deployment of the solution in existing networks with current equipments. In addition, we also use an auto-configuration protocol which provides nodes with topologically correct IP addresses and reduces network overhead by the use of *prefix continuity*. That is, all wireless routers using the same Internet gateway are configured with addresses on the same prefix. Our simulation and empirical results in a real testbed show that the proposed scheme is able to offer a good performance, while being fully compatible with standardized multicast solutions for fixed networks.

The remainder of the paper is organized as follows: Section II presents some of the related work on address auto-configuration and multicast routing in ad hoc networks. Section III describes the concept of prefix continuity and the proposed multicast routing protocol, which are the central elements of our proposal. In section IV we explain how these protocols are integrated to provide the full solution. Section V gives some simulations results to evaluate multicast routing based on prefix continuity. Section VI shows the performance of the protocols in a real testbed. Finally, section VII provides some conclusions and final comments.

II. Related Work

We analyze relevant literature on the two main components of our solution: the creation of default multicast routes towards the Internet based on an auto-configuration solution, and the routing scheme within the WMN.

A. Address auto-configuration

The applicability of IPv6 auto-configuration mechanisms to ad hoc networking has been investigated in some papers. The adoption of the IPv6 Stateless Address Autoconfiguration (SAA) and the corresponding Neighbour Discovery Protocol (NDP) is proposed in [1]. However, these mechanisms were designed to work on a shared broadcast link, and the changes required to make it work over multihop wireless networks do not preserve their original simplicity and efficiency. Thus, we believe that the use of such techniques should be avoided for wireless multihop networks.

Among the mechanisms specially designed to provide Internet connectivity to ad hoc networks, we can distinguish the method proposed by Wakikawa *et al*. [2]. They proposed a stateless auto-configuration mechanism based on network prefixes advertised by gateways. Ad hoc nodes concatenate an interface identifier to one of those prefixes in order to generate a unique IPv6 address. Wakikawa defines two gateway discovery mechanisms: a reactive and a proactive one. The reactive version utilizes solicitation and advertisement signaling between the ad hoc node and the gateway. The proactive approach is based on the periodic flooding of gateway advertisement to all the nodes in the MANET. They also perform a *Duplicate Address Detection* (DAD) process that does not work when network partitions and merges occur. Additionally, this scheme shortly introduces the notion of gateway selection, but it does not give details about how this would be achieved. Singh *et al.* [3] introduced a new scenario where gateways are mobile nodes which are one hop away from a wireless access router. Nodes employ a hybrid gateway discovery scheme, since they can request gateway information or receive it proactively. The first node which becomes a gateway is known as the *default gateway*, and it is responsible for the periodic flooding of gateway messages. Remaining gateways are called *candidate gateways* and they only send gateway information when they receive a request message. Nevertheless, this scheme does not manage the situation where several network prefixes are advertised by different access routers.

A broader discussion and analysis of existing solutions and their trade-offs can be found in [4]–[6]. However, most of these solutions do not guarantee that addresses are always topologically correct.

B. Multicast within the WMN

IP multicast protocols used in the Internet (i.e. MLD [7] for multicast group membership and PIM-SM [8] for IP multicast routing) can not be used within ad hoc networks due to the high overhead that they require to react to continuous topological changes. Even for WMNs, which are static, these protocols are not able to take advantage of the broadcast nature of the wireless channel (i.e. a single transmission can be used to reach all children in the multicast tree). Hence, they provide sub-optimal solutions, and are not quite well-prepared to deal with mobility of end hosts.

Special routing mechanisms have been engineered to achieve efficient multicasting support in ad hoc networks. Many of them have been defined as an extension of unicast ad hoc routing protocols, but most of them have been specially designed for multicast.

In the first group, we can find an extension to the unicast Ad Hoc On-Demand Distance Vector (AODV) proposed under the name of MAODV [9]. The implementation of a gateway between MAODV as the ad hoc routing protocol and MOSPF [11] as the infrastructure routing protocol is described in [10]. They limit the implementation to these protocols and they propose to design similar solutions for other protocols. In addition, it requires modifications in both MAODV and OSPF implementations running in the gateway. The MOLSR [12] protocol presents a multicast extension for the OLSR protocol. MOLSR introduces a Wireless Internet Group Management Protocol (WIGMP) which offers the possibility for OLSR nodes (without multicast capabilities) to participate in multicast communications. One inconvenient of this protocol is that it requires the OLSR unicast routing protocol. In addition, it does not incorporate any mechanism for interconnecting to the Internet.

Examples of multicast ad hoc routing protocols in the second group are CAMP [13], ODMRP [14] and ADMR [15]. None of these protocols provide any means to interoperate with the protocols used in fixed IP networks and they do not support the attachment of standard IP multicast nodes to the ad hoc network.

The first multicast routing solution for ad hoc networks supporting an efficient interworking with fixed IP networks was introduced by Ruiz et. al [16]. It uses a multicast mesh to route packets within the MANET while supporting high mobility rates. In addition, it uses standard group membership mechanisms so that ad hoc nodes can interact both with traditional wired IP multicast routing protocols as well as standard IP multicast hosts. However, when the network is static, there is no need to use a mesh, and data overhead can be reduced by using a cost-efficient multicast tree.

Our solution preserves MMARP's interoperability procedures, while using a new enhanced low data-overhead multicast tree construction much better suited for wireless mesh networks.

III. Requirements and technical issues

Typical wireless mesh network deployments use one or multiple gateways to provide Internet connectivity to mobile end hosts. This means that maintaining interoperability with protocols used in the Internet is a must, as long as it is not feasible in the short term to change the Internet architecture to support this kind of access networks. However, being fully interoperable while efficiently supporting multicast traffic is very challenging, and requires new protocols and mechanisms within the WMN. In this section we describe and analyze those technical challenges in detail.

In particular, we start by defining the technical requirements that should be expected from any suitable solution.

- Globally routable and unique addresses. Internet gateways must provide globally routable prefixes, and ad hoc nodes must ensure address uniqueness. Address uniqueness is key to guarantee the correct operation of routing protocols. Global routability is required for multicast routers in the Internet to be able to create multicast routes towards multicast sources in the MANET. For instance, the most common routing protocol (PIM-SM) uses unicast routes to join multicast receivers back to the source.
- Interoperability with the Internet. The proposed mechanisms should interoperate with the protocols used in Internet. This requirement is twofold: routers in the fixed network should be able to continue using the same routing protocols, and they should be able to continue using the same group membership protocol. Moreover, the proposed solution should be effective regardless of the standardized multicast routing protocol being used in the Internet.
- Effective multicast routing within the ad hoc fringe. Internal ad hoc routing mechanism should be efficient, scalable, robust and with low signaling overhead. That is, the wireless part of the network has a lower amount of resources compared to high-bandwidth wireline networks. Thus, the routing protocol deployed within the wireless mesh must be really efficient in terms of low control overhead, and high bandwidth efficiency.
- Resilience. The proposed scheme should be fully distributed and must provide resilience to bandwidth changes of the wireless links. In addition, several gateways should be supported to eliminate single points of failure. Hence, the addressing scheme should be able to support multiple gateways while guaranteeing that *RPF Checks* performed by access routers are still valid.

Supporting those requirements means that some technical challenges need to be faced in order to offer an smooth interoperation with multicast protocols in the fixed network. First of all, addresses assigned to mobile nodes need to be topologically correct. So that *RPF checks* are successful at access routers. To address this lack, we use a mechanism introduced by Jelger *et al.* [17] called *prefix continuity*. In short, prefix continuity feature ensures that there exists, between a node N and its gateway G, a path of nodes such that each node on this path uses the same prefix P and gateway G than the node N. We detail this mechanism within the next section.

Group membership messages use a maximum TTL of one hop. Thus, they need to be handled so that standard multicast host situated many hops away from access routers can still be able to join multicast sessions. The option of flooding group membership queries and replies over multiple hops is not really effective as it requires a lot of control overhead. Our solution is based on the idea introduced by Ruiz [16], by which mesh nodes interact with standard IP nodes and multicast routers using those standard MLD or IGMP messages, but use their multicast routing messages based on the membership information obtained.

Another important aspect to consider, is that existing intra and inter-domain (e.g. PIM-SM) multicast routing protocols require knowing the address of multicast sources. In wired networks, the access router is always one hop away from sources, thus it receives multicast messages and can notify using routing messages about that IP address. That means that in the wireless mesh network, we must guarantee that the multicast router which is best for this source joins the multicast group. Hence, the efficiency of the created multicast path between the gateway and sources in the mesh is of utmost importance. That is the reason why we use prefix continuity and evaluate the properties of trees based on prefix continuity within the next sections.

IV. Proposed solution

We describe in this section the different components of our proposed solution. Firstly, we will describe the gateway discovery scheme based on prefix continuity and how default multicast routes towards gateways are created. Then, we will explain in detail how is interoperability achieved. Finally we will describe how the multicast routing within the mesh works.

A. Internet gateway discovery

There might be cases where multicast delivery structures should be formed by nodes using the same network prefix than their gateway and different from nodes using other gateways. For example, a network or service provider could restrict the access to multicast streaming to nodes that have registered (and possibly paid a fee) with its gateway.

To support those scenarios we can use the approach introduced by Jelger *et al.* [17], which defined the concept of *prefix continuity* in a MANET. When prefix continuity is preserved, there is a guarantee that there exists a path of nodes between a node N and its gateway G such that each node on this path uses the same prefix P and gateway G than the node N. In practice, in a network with multiple gateways and multiple prefixes, this concept results in the proactive creation of a forest of logical spanning trees where each tree is formed by nodes using the same gateway/prefix pair. This is illustrated by Fig. 1 which shows a hybrid ad hoc network with (a) and without (b) prefix continuity. There are 3 gateways, and each color corresponds to a given network prefix. Moreover, each logical tree is oriented (or directed) from the gateway to the leaf nodes, as shown in Fig. 1a with arrows. Also note that while each sub-network is actually created as a logical tree, the physical topology of a sub-network can be of any kind (e.g. a mesh) and routing inside the wireless network does not necessarily follow the tree structure. A detailed description of the protocol used to achieve prefix continuity can be found in [17].

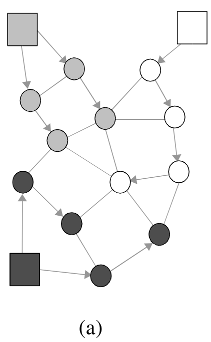


Fig. 1. Ad hoc network with (a) and without (b) prefix continuity

We present some mechanisms that can be used to build multicast structures (i.e. trees or meshes) which are based on prefix continuity. That is, when there are multiple sub-networks in an ad hoc network, each multicast delivery structure is formed by nodes which all share an identical prefix. Communication between trees using different prefixes is done via the gateways. One must note that the purpose of our proposal is to *add* members to the tree, i.e. we only focus on how the multicast structure is built. Once nodes are added to this structure, one can arbitrarily decide to create a tree or a mesh by simply choosing if forwarding is restricted or not. Moreover, for simplicity and in the rest of this paper, we will use the term *tree* to refer to the *multicast structure*. One must however remind that this *so-called tree* could also become a mesh if there is no restriction on multicast data forwarding.

An example of a multicast tree based (a) or not based (b) on prefix continuity is shown on Fig. 2. This example represents a shared tree or a source-rooted tree, i.e. the root is either some sort of central point or the source of the group.

Note that in the two cases prefix continuity is used to configure the nodes addresses. In the first case, prefix continuity is also used to restrict the construction of the multicast tree. That is, a branch cannot be built between a node and the root if they do not share the same prefix. Therefore some branches are built towards the gateways, and communication between the gateways is done via the multicast routing protocol that is used in the wired network. In the second case, a shortest-path tree is built between all group members and the root of the tree. Note that the tree members are the same whether a tree or a mesh structure is built. The difference lies in the number of edges.

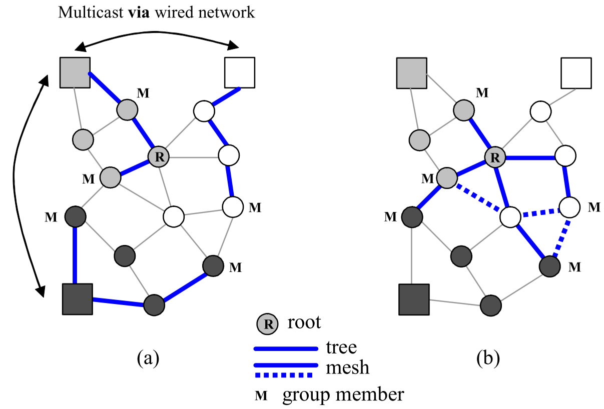


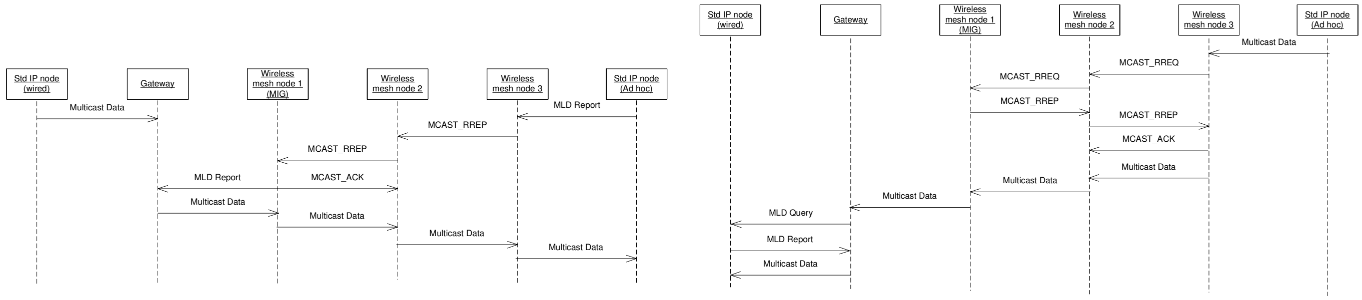
Fig. 2. Multicast tree based (a) and not based (b) on prefix continuity

The advantages of multicast routing based on prefix continuity is that management and control operations can easily be implemented in the gateways. For example, it is easily possible to control which groups can be accessed via a given gateway. Moreover, the transit of multicast data between two sub-networks via a third (or more) sub-network is forbidden. This restriction allows saving resources (e.g. bandwidth, energy) in ad hoc nodes and it also ensures that any filtering done by the gateway cannot be bypassed. Finally, in Section V we also show via multiple simulations that the characteristics of multicast trees based on the concept of prefix continuity are very similar from those of shortest-path trees.

B. *Detailed interworking with access routers*

Fig. 3 shows the interaction of the protocol in two scenarios: when a source is in the ad hoc fringe and the receiver in the Internet and the opposite case. The Gateway is a standard multicast-enabled router running PIM-SM. Wireless mesh nodes are wireless routers running our bandwidth efficient multicast path creation scheme and the IP nodes are standard Internet hosts. One of the IP nodes is in the wired network and the other one is connected to the wireless mesh.

The interoperation with gateways is performed by wireless mesh nodes which have direct connectivity to access routers. We call them MIGs (Multicast Internet Gateways). The reception of an MLD Query or IGMP Query message can be used by those nodes to detect that they must act as MIGs. If that is the case, they must send IGMP or MLD reports to the access router, to inform about which multicast groups have interested receivers within the mesh. MIGs know this information because receivers within the mesh will send IGMP or MLD reports to their selected wireless mesh node, which will in turn create a multicast path towards the gateway following its best path towards the gateway based on prefix continuity. Of course, those paths are created in advance by the periodic gateway advertisements explained before and all



(a) Source in the ad hoc fringe

(b) Receiver in the ad hoc fringe

Fig. 3. Interworking with fixed network

wireless mesh nodes know their parent in the prefix continuity tree.

The MIG is also responsible for joining all the multicast groups with active senders within the wireless mesh and to forward all the multicast traffic towards the gateway so that it can detect that sources and execute the IP multicast routing specific functions. This mechanism allows MMARP's solution to work with any IP multicast routing protocol in the fixed network.

C. Multicast routing within the WMN

To perform efficient multicast routing within the wireless mesh network, we use an epidemic algorithm which is able to approximate multicast trees in which data overhead is minimal. This scheme builds upon the work published by Ruiz [18], but rather than creating multicast spiders, it just focus on the approximation of the minimal data-overhead paths. The reason is that given that end host will be connected to their selected wireless mesh node, that automatically guarantee that they form an optimal spider.

To build a Steiner tree among the roots of the subtrees, the previous protocol used the MST heuristic. However, this is a centralized heuristic consisting of two different phases. Firstly, the algorithm builds the metric closure on the whole graph, and then, a minimum spanning tree (MST) is computed on the metric closure. Finally, each edge in the MST is substituted by the shortest path tree between the to nodes connected by that edge. Unfortunately, the metric closure of a graph is hard to build in a distributed way. However, we can approximate such an MST heuristic with the simple, yet powerful, algorithm presented in the algorithm below. The source, or the root of the subtree in which the source is (called source-root) will start flooding a route request message (MCAST_RREQ). Intermediate nodes, when propagating that message will increase the hop count. When the MCAST_RREQ is received by a root of a subtree, it sends a route reply (MCAST_RREP) back through the path which reported the lowest hop count. Those nodes in that path are selected as multicast forwarders (MF). In addition, a root of a subtree, when propagating the MCAST_RREQ will reset the hop count field. This is what makes the process very similar to the computation of the MST on the metric closure. In fact, we achieve the same effect, which is that each root of the subtrees, will add to the Steiner tree the path from itself to the source-root, or the nearest root of a subtree. The way in which the algorithm is executed from the source-root to the other nodes guarantees that the obtained tree is connected.

Algorithm 1 Distributed approximation of MST heuristic

if $thisnode.id = source - root$ **then**
  Send MCAST_RREQ with MCAST_RREQ.hopcount=0
end if
if rcvd non duplicate MCAST_RREQ with better hopcount **then**
  prevhop $\leftarrow$ MCAST_RREQ.sender
  MCAST_RREP.nexthop $\leftarrow$ prevhop
  MCAST_RREQ.sender $\leftarrow$ $thisnode.id$
  if $thisnode.isroot$ **then**
    send(MCAST_RREP)
    MCAST_RREQ.hopcount $\leftarrow$ 0
  else
    MCAST_RREQ.hopcount++;
  end if
  send(MCAST_RREQ)
end if
if received MCAST_RREP and MCAST_RREP.nexthop = $thisnode.id$ **then**
  Activate MF_FLAG
  MCAST_RREP.nexthop $\leftarrow$ prevhop
  send(MCAST_RREP)
end if

The support of standard IP nodes is performed allowing mesh nodes in the neighbourhood of a standard IP node to behave as a multicast source in the wireless mesh. To support standard-IP receivers, the selected wireless mesh node of the receiver takes care of sending an MCAST_RREP message towards the source.

Within the next sections we evaluate the performance of the proposed schemes using both simulations and empirical measurements.

V. SIMULATION ANALYSIS

In order to evaluate the impact of prefix continuity on multicast trees, we have compared the topological characteristics of such trees with shortest-path trees (which are not based on prefix continuity). We used the NS-2 simulator with the IEEE 802.11 protocol in ad hoc mode. We have simulated the construction of multicast trees with 5 to 50 group members, with different ad hoc topologies of 125 nodes. We have made sure to obtain representative results, i.e. the results presented in this section have a very low confidence interval for a very high confidence level (i.e. 95% of the data is comprised within $\pm$5% of the associated average value).

Moreover we have considered two different *frames* for the topologies. The first frame is a square topology with 4 gateways located at the corners of the square. The second frame is a rectangle of size 1000×4000 m^2, with 100 mobile nodes with a 250 meters radio range. The area (4 km^2) is the same than with the square topology so that node density is comparable. Also, there are again 4 gateways, which are located at the center of the 4 squares of size 1000×1000 m^2 that form the rectangle. Each gateway announces a different prefix. In the remaining of this paper, we will refer to these two architectures with the terms SQUARE and LINE. These two network configurations could for example represent a large hall or a long corridor with fixed gateways (e.g. an exhibition hall in which visitors are equipped with a personal digital assistant that receives a multicast video stream).

A. *Average size of multicast trees*

We have first focused on the average size of the multicast trees, i.e. the number of nodes in a tree. It is well accepted that the size of multicast trees in the Internet follows a power-law which was first discovered by Chiang and Sirbu in [19]. This power-law is given as

$$L_m = \overline{L_u} N^k \tag{1}$$

where L_m is the number of links (or nodes-1) in the multicast tree, $\overline{L_u}$ is the average unicast path-length in the considered topology, and N is the size of the multicast group in terms of routers with group members. The value k is known as the multicast scaling factor ($k \in [0, 1]$). In [19], this value is found to be constant and equal to 0.8 across a wide range of topologies and group members. In other studies such as [20], the value of k is found to be closer to 0.7 (but with more recent Internet topologies when compared to [19]). Moreover, another study [21] has shown that k is not a constant but that it rather slowly increases from 0.71 to 1 with N (with values of N of 1,000 and more).

Fig. V-A shows the average size T of multicast trees with respect to the number of group members N (i.e. receivers and/or sources). Note that we only consider ad hoc nodes, when trees based on prefix continuity also involve routers from the wired part of the network. We indeed only consider ad hoc nodes because they are limited in resources, while we can reasonably assume that routers in the *wired network* have access to much more bandwidth and processing power.

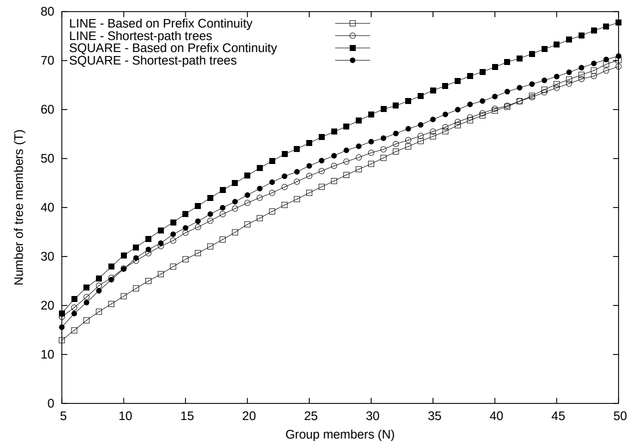


Fig. 4. Average size of multicast trees

First, one can note that the maximum difference between shortest-path trees and trees based on prefix continuity is roughly equal to 8 nodes. This is very interesting, as trees based on prefix continuity do not involve more members in the ad hoc network. Moreover, with the LINE configuration, these trees involve less ad hoc nodes when compared to shortest-path trees and with $N < 40$. We have also found that the four curves can be modeled by a power-law given as

$$T = \alpha N^k \tag{2}$$

which has the same form than the Chuang-Sirbu power-law given by (1). Actually, we have derived the values of α and k that best fit these curves, and we have also derived k if $\alpha = \overline{L_u}$ (i.e. the strict form of the Chuang-Sirbu power-law). These values are given in Table I.

	Exact values		With $\alpha = \overline{L_u}$	
	α	k	$\overline{L_u}$	k
LINE - Prefix continuity	4.2	0.72	6.26	0.61
LINE - Shortest-path	7.4	0.57	6.26	0.62
SQUARE - Prefix cont.	7.9	0.59	5.41	0.69
SQUARE - Shortest-path	7.2	0.59	5.41	0.67

TABLE I
POWER-LAW PARAMETERS

It can be seen that the values of k when $\alpha = \overline{L_u}$ are very close between the two types of trees for each network configuration (LINE and SQUARE). Actually these equations are not the best fit but surprisingly the value of k does not seem to be strongly influenced by the method used to build the multicast trees. One explanation could be that the Chuang-Sirbu law seems to be more accurate with large multicast groups and topologies. Maybe with larger groups and topologies the

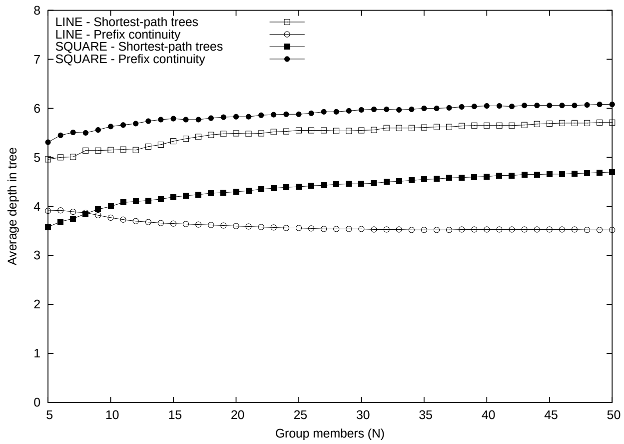


Fig. 5. Average depth of multicast trees

equations following the Chuang-Sirbu power-law would be the best fit. Also one can note that k is comprized beetween 0.61 and 0.69, i.e. slightly smaller values than what was found in studies with (relatively) large Internet-like topologies. This could validate the fact that k varies with the size of multicast groups and network topologies [21].

B. Average depth of multicast trees

The second indicator that we used to compare the trees is the average depth of tree members. Of particular interest, it indicates the distance at which tree members are located from the root of a tree. If the depth is high, a lot of packet forwarding is necessary to reach the group members. This increases the packet delivery delay and the overall energy required to reach group members. This data is shown in Fig. V-B.

With the SQUARE network configuration, the average depth is higher with trees based on prefix continuity while it is smaller with the LINE configuration. This is consistent with the nature of the configurations. The average unicast path-length (i.e. $\overline{L_u}$) is indeed longer with LINE topologies than with SQUARE topologies (see Table I for details). Therefore shortest-path trees are deeper with the LINE configuration. In opposition, trees based on prefix continuity are deeper with the SQUARE configuration. This is mainly due to the fact that gateways are placed at the corner of the simulated area, and thus at (in average) longer distances from mobile nodes when compared to the LINE configuration.

A more pertinent conclusion is that the placement of gateways strongly affects this indicator for multicast trees based on prefix continuity. However, one can always find positions for gateways in order to minimize the average depth of multicast trees, whatever group members and tree size. It is also interesting to node that the average depth is not strongly influenced by the number of group members. The average depth of multicast trees is indeed rather influenced by topological issues, i.e. it merely depends on the spatial distribution of nodes.

C. Average noise caused by multicast trees

In many studies on the shape and the efficiency of multicast trees, some attention is given to the nodes *tree-degree*. For each node that is part of a multicast tree, the tree-degree of a node is defined as the number of the node's neighbors that are also members of the same multicast tree. From a practical aspect with wired networks, the tree-degree is also related to the number of packet duplication done by a tree member : a node must forward a copy of a multicast packet to all of its neighbors in the tree (excepting the node from which the data is received). This is usually because links between routers in wired networks are point-to-point links. In contrast, in ad hoc networks communication is done via a broadcast medium (for a given interface). Therefore a node that is a member of a multicast tree only needs to re-broadcast a multicast packet once in order to reach all its tree-neighbors. (strictly speaking this is only valid for each network interface). This advantage (i.e. only on packet forwarding) is also a disadvantage: all the neighbors which are not members of a multicast tree will also be affected by the forwarding of multicast data. The forwarding of multicast data can indeed prevent non-tree members from accessing the shared medium (assuming that they have neighbors which are members of one or multiple multicast trees). We define this effect as the *noise* of a multicast tree. We believe that this indicator is very important in ad hoc networks, mainly because multicast communications with high data rates can strongly affect the throughput of some nodes.

We have therefore measured the average noise of a multicast tree by counting, for each member of a multicast tree, the number of neighbors (of each tree member) that were not part of the multicast tree. This is presented in Fig. V-C.

It can be seen on Fig. V-C that the noise is very similar between shortest-path trees and trees based on prefix continuity (for each network configuration). In all cases, the average noise decreases when the size of the group increases, mainly because more nodes are added to the tree. The main conclusion

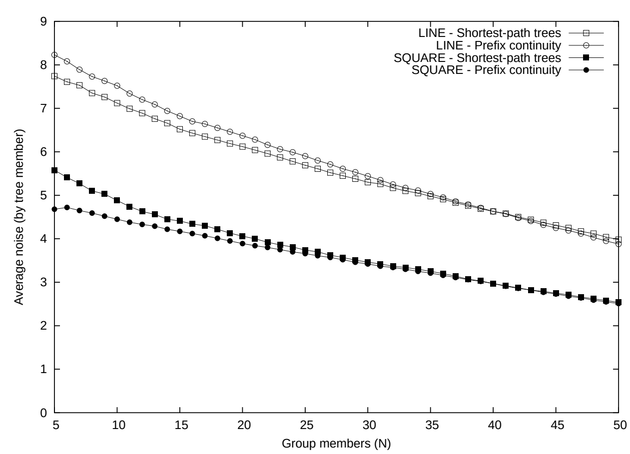


Fig. 6. Average noise caused by multicast trees

is that the negative impact of multicast trees (in terms of access probability to the transmission medium) is similar with shortest-path trees and trees based on prefix continuity.

D. *Forwarding states concentration*

In this part we have studied the concentration of forwarding states in the nodes of the ad hoc network. When there are multiple multicast groups, some nodes may indeed have a lot of forwarding states, i.e. one forwarding state for each group they belong to. There are a number of negative consequences when an ad hoc node has a lot of multicast forwarding states. First, such a node will have to forward a lot of multicast packets : this consumes a lot of energy and bandwidth. Second, such a node will be very *noisy*, and may strongly reduce the bandwidth available for its neighbors. Third, the failure of such a node can seriously interrupt the data forwarding of many multicast groups.

In our simulations, we have studied the concentration of forwarding state with up to 50 multicast groups. The set of members for each group has been randomly and uniformly chosen among the nodes of the ad hoc network. The size of each multicast group is 50 (large groups with respect to the total number of nodes in the network). We used large groups on purpose in order to exacerbate the effect of forwarding states concentration. Fig. V-D and V-D present some of these results for 5, 25 and 50 concurrent multicast groups (G), with shortest-path trees (SP) and trees based on prefix continuity (PC). Results are presented in the form of survival functions, i.e. it gives the percentage of nodes that have more than S forwarding states.

A first conclusion is that results are (globally) quite close between shortest-path trees and trees based on prefix continuity. There is however a slight difference for $G = 25$ and $G = 50$ when $S < 15$. It mainly means that there are less nodes with few forwarding states with trees based on prefix continuity when compared to shortest-path trees. With $S > 25$, the configuration of the network (i.e. LINE or SQUARE) has a clear influence on the results.

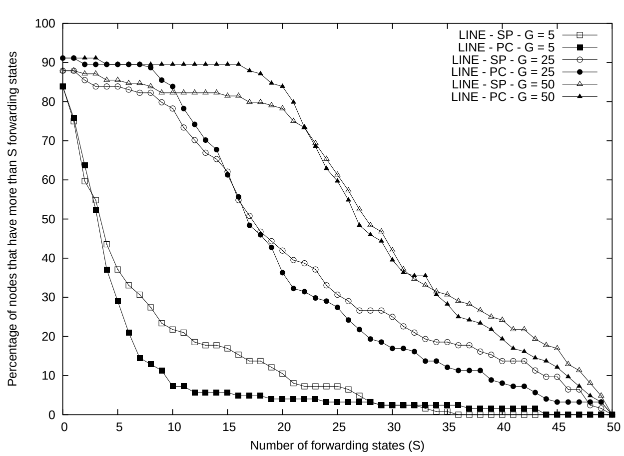


Fig. 7. Forwarding states concentration with a LINE configuration

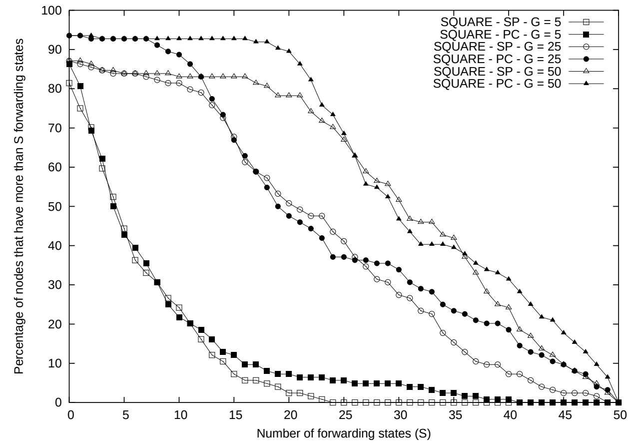


Fig. 8. Forwarding states concentration with a SQUARE configuration

One should actually remind that the Chuang-Sirbu power-law says that we can derive the number of members of a multicast tree if the size of the multicast group is known. Building from previous studies [19]–[21] and from Section V-A, we can say that one can always derive a k parameter in order to fit the power-law to a given network topology. Therefore, it is always possible to know how many forwarding states will be *applied* to the network. The number of tree member and the number of forwarding states are indeed *equivalent*, i.e. when a node is added to a multicast tree one forwarding state is added in the network. As a result, if G multicast groups of size N are considered, there will always be $\overline{L_u}N^k$ forwarding states to *be applied* to the network.

The main difference lies in the way these forwarding states are distributed in the network. With trees based on prefix continuity, each gateway and its neighbors will have a large proportion of forwarding states. This is because a branch between a group member and a root which use different prefixes will always be routed via the node's gateway and the root's gateway. On the other hand with shortest-path trees, it can be seen on Figures 12 and 13 that there are also nodes that have a large proportion of forwarding states. One explanation is that these nodes are *at the center* of the topology, i.e. they have a high probability to be on a unicast path between any two nodes. They are therefore in most of the multicast trees, regardless of the group members.

VI. Performance Evaluation

We have set up an indoor 802.11b multicast wired-to-wireless ad hoc network testbed to evaluate the performance of our seamless IP multicast approach for wireless mesh access networks. Our target is to evaluate the benefit of using *prefix continuity* in a real scenario in terms of packet delivery ratio and control overhead.

A. *Testbed description*

The testbed consists of twelve PCs running Mandrake Linux 10.0 with kernel 2.6.3-7. Ten of these PCs are acting as wireless mesh nodes, and the other two are acting as gateways between the wired and wireless networks. Gateways can establish a multicast communication through the wired network using the PIM-SM multicast routing protocol.

Wireless cards are Lucent-compatible PCMCIA 802.11b Wireless LAN operating in ad hoc mode at the maximum capacity of 2 Mb/s. We previously checked that the wireless channel used was not occupied by any other equipment.

B. Description of the experiments

The goal of the experiment is to assess the effectiveness of the prefix continuity approach in a multicast communication. The topology used is shown in Fig. 9. When prefix continuity approach is used, the MANET is split into two areas, having the same gateway/prefix pair in each area. Multicast source and receivers have different prefixes and consequently the communication is performed via the wired network. The wired part of the network is running the PIM-SM multicast routing protocol to create the multicast path between the gateways. Without prefix continuity, the communication is performed always inside the MANET.

The multicast source is placed in the middle of one of these areas in all the experiments; three hops away to its gateway, and the same distance to nodes with different prefix. Meanwhile, the position of the receiver oscillate in each experiment. It is important to understand that the best results with prefix continuity are obtained when the receiver is placed near to its gateway (seven hops far to the sender), because the communication is performed via wired network, but without prefix continuity the best behavior is obtained when the receiver is located near to the sender (three hops away), because they communicate through the MANET.

We use a constant bit rate traffic generator application to measure the packet delivery ratio and the normalized overhead. This application generates UDP packets with a payload of 1144 bytes (i.e. 1.200 bytes including the IPv6 and UDP headers). We have performed several measures at increasing distances (3 hops, 4 hops, 5 hops, 6 hops and 7 hops) between the source and the receiver. At each distance, we have repeated the measurements using two different data rates of 100Kb/s and 200Kb/s. The results of the different trials are described in the next section.

C. Experimental results

The performance metrics we use to determine the convenience of the prefix continuity approach are the packet delivery ratio and the normalized overhead. Fig. 10 shows the packet delivery ratio for the two data rates used with and without prefix continuity approach. The results are basically the expected: Without prefix continuity, the packet delivery ratio decreases when increasing the distance between the source and the receiver. Using prefix continuity, the packet delivery ratio decreases when the distance between the receiver and its gateway increases. The differences between both approaches are easier to appreciate with the higher data rate. It can be noticed that the performance with prefix continuity at

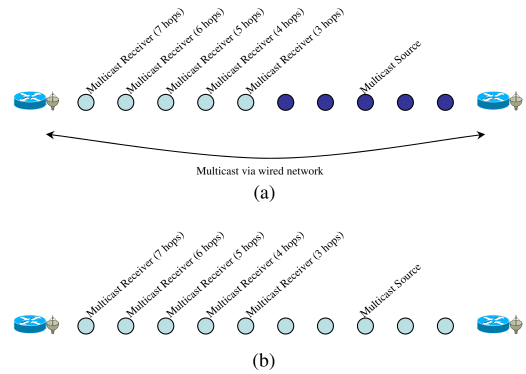


Fig. 9. Testbed based (a) and not based (b) on prefix continuity

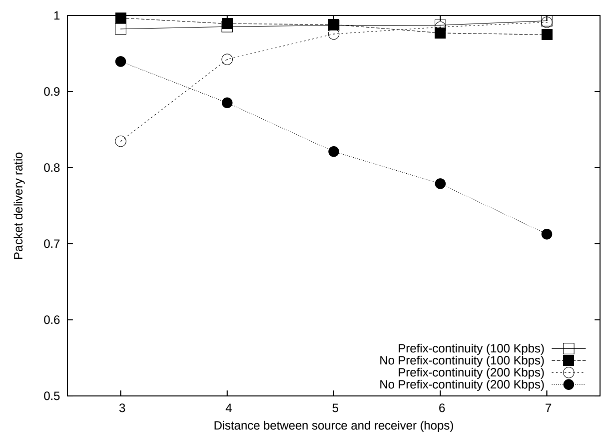


Fig. 10. Packet delivery ratio

increasing distances degrades too much slower than without prefix continuity. The reason is that the overall load on the network is much lower, as well as the fact that the number of wireless (eventually prone to errors) links traversed is reduced.

It is very interesting to observe the trial with the receiver located in the middle of the its prefix area and a data rate of 200Kb/s. The multicast traffic without prefix continuity requires five wireless hops to arrive to the receiver and with prefix continuity requires six wireless hops and the wired communication between the gateways. The packet delivery ratio with prefix continuity is closer to 0.98 whereas without prefix continuity the packet delivery ratio is 0.82. There are two reasons for this reduction in packet delivery ratio. The first one is that traversing a lower number of wireless links reduced the probability of packet losses, and of course the lower traffic load incurred by the prefix continuity approach (each gateway only floods part of the network) also reduces the probability of losses due to collisions, interference, etc.

Normalized overhead is the number of control bytes transmitted per data byte received at the destination. We count both gateway discovery traffic as well as routing messages as control overhead. Fig 11 shows the normalized control overhead introduced by the ad hoc protocols. We can observe that the overhead is greater with lower data rates. The reason is

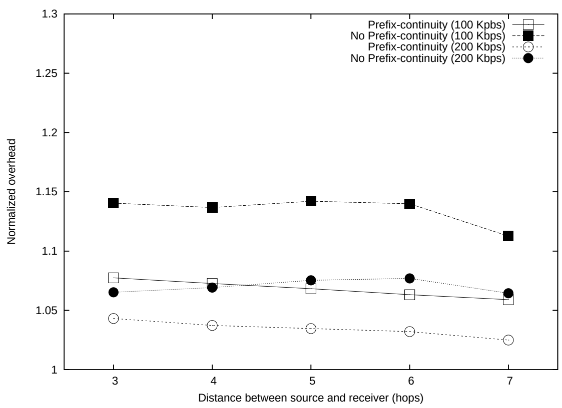


Fig. 11. Normalized overhead

that the overhead introduced by the multicast routing protocol is independent of the data rate, though if there is no communication then there are no control messages generated in the network. We can appreciate the difference of overhead when prefix continuity is used. The reason is the that control packets are only flooding within their prefix area. The limitation of control messages flooding to their prefix area has probed to be very effective in ad hoc networks where the bandwidth is scarce and the mobility of the nodes requires frequent flooding of control packets.

VII. Conclusion and Future Work

We have presented an integrated solution for efficiently supporting multicast communications in wireless mesh networks. Three are three key components of the proposed solution: the mechanism to autoconfigure addresses and creation of default routes, the interworking with fixed networks and an efficient multicast routing within the multicast mesh. Our solution is able to be deployed with existing routing protocols and devices.

The auto-configuration scheme is based on the idea of prefix continuity. This solution is particularly interesting for wireless mesh networks because it allows for a reduction on the control overhead. Moreover, the prefix continuity paradigm has another very interesting feature for multicasting, which is the fact that addresses are topologically correct, making it easier for routing protocols to interoperate. In addition, the proposed tree creation scheme based on the reduction of the data overhead allows our proposed scheme to build really efficient multicast trees in terms of the overall bandwidth consumption.

Our simulation and experimental results show that the creation of default routes based on prefix continuity, lead to multicast trees which are similar in properties to source path trees. In addition, our experiment have shown that the use of prefix continuity greatly reduces the amount of control overhead in the network and it enhances the overall packet delivery ratio.

Acknowledgment

Part of this work has been funded by the *Ramon y Cajal* workprogramme and the SMART (TIN2005-07705-C02-02) project.

References

[1] K. Weniger and M. Zitterbart, "IPv6 autoconfiguration in large scale mobile ad-hoc networks," in *Proceedings of European Wireless Conference*, February 2002.

[2] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, and A. Tuominen, "Internet connectivity for mobile ad hoc networks," *Wirel. Comm. and Mobile Computing*, vol. 2(5), pp. 465–482, August 2002.

[3] S. Singh, J. H. Kim, Y. G. Choi, K. L. Kang, and Y. S. Roh, "Mobile multi-gateway support for IPv6 mobile ad hoc networks," Internet Draft draft-singh-manet-mmg-00, June 2004.

[4] S. Singh, J. Kim, C. Perkins, T. Clausen, and P. Ruiz, "Internet Draft - Ad hoc network autoconfiguration: definition and problem statement, draft-singh-autoconf-adp-02," Internet Draft draft-singh-autoconf-adp-02, February 2005.

[5] K. Weniger and M. Zitterbart, "Address Autoconfiguration in Mobile Ad hoc Networks: Current Approaches and Future Directions," *IEEE Network*, vol. 18, no. 4, pp. 6–11, July 2004.

[6] A. G.-S. P. Ruiz, F. Ros, "Internet Connectivity for Mobile Ad Hoc Networks: Solutions and Challenges," *IEEE Communications Magazine*, vol. October 2005, pp. 118–125, July 2005.

[7] S. Deering, W. Fenner, and B. Haberman, "Multicast listener discovery (MLD) for IPv6," RFC 2710, October 1999.

[8] D. Estrin, D. Farinacci, A. Helmy, D. Thaler, S. Deering, M. Handley, V. Jacobson, C. Liu, P. Sharna, and L. Wei, "Protocol independent multicast sparse mode (PIM-SM): Protocol specification," RFC 2362, June 1998.

[9] E. Royer and C. Perkins, "Multicast operation of the ad hoc on-demand distance vector routing protocol," in *Proceedings of ACM Mobicom*, August 1999, pp. 207–218.

[10] J. McGee, M. Karir, and J. Baras, "Implementing ad hoc to terrestrial network gateways," in *Proceedings of Wired/Wireless Internet Communications (WWIC)*, 2004, pp. 132–142.

[11] J. Moy, "Multicast extension to OSPF," RFC 1584, March 1994.

[12] A. Laouiti, P. Jacquet, P. Minet, L. Viennot, T. Clausen, and C. Adjih, "Multicast optimized link state routing," INRIA Rocquencourt, Tech. Rep., February 2003. [Online]. Available: ftp://ftp.inria.fr/INRIA/publication/publi-pdf/RR/RR-4721.pdf

[13] J. Garcia-Luna-Aceves and E. Madruga, "The core assisted mesh protocol," *IEEE Journal on Selected Areas in Communications, Special Issue on Ad-Hoc Networks*, vol. 17(8), pp. 1380–1394, August 1999.

[14] S.-J. Lee, M. Gerla, and C.-C. Chiang, "On demand multicast routing protocol," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, September 1999, pp. 1298–1304.

[15] J. G. Jetcheva and D. D. Johnson, "Adaptive demand-driven multicast routing in multi-hop wireless ad hoc networks," in *Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing*, 2001, pp. 33–44.

[16] P. M. Ruiz, A. F. Gomez-Skarmeta, and I. Groves, "The MMARP protocol for efficient support of standard ip multicast in mobile ad hoc access networks," in *Proceedings of the IST Mobile and Wireless Communications Summit 2003*, June 2003, pp. 478–482, Aveiro, Portugal.

[17] C. Jelger and T. Noel, "Proactive Address Autoconfiguration and Prefix Continuity in IPv6 Hybrid Ad Hoc Networks," in *Proceedings of IEEE SECON'05*, September 2005, Santa Clara, CA, USA.

[18] P. M. Ruiz and A. F. Gomez-Skarmeta, "Approximating optimal multicast trees in wireless multihop networks," in *Proceedings of the IEEE ISCC 2003*, June 2003, pp. 686–691, La Manga, Spain.

[19] J. Chuang and M. Sirbu, "Pricing Multicast Communications: A Cost Based Approach," in *Proceedings of INET'98*, July 1998.

[20] R. Chalmers and K. Almeroth, "On the Topology of Multicast Trees," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 153–165, February 2003.

[21] P. V. Mieghem, G. Hooghiemstra, and R. V. D. Hofstad, "On the Efficiency of Multicast," *IEEE/ACM Transactions on Networking*, vol. 9, no. 6, pp. 719–732, December 2001.