Routing and Broadcasting in Hybrid Ad Hoc Networks

François Ingelrest, David Simplot-Ryl, Ivan Stojmenovic

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

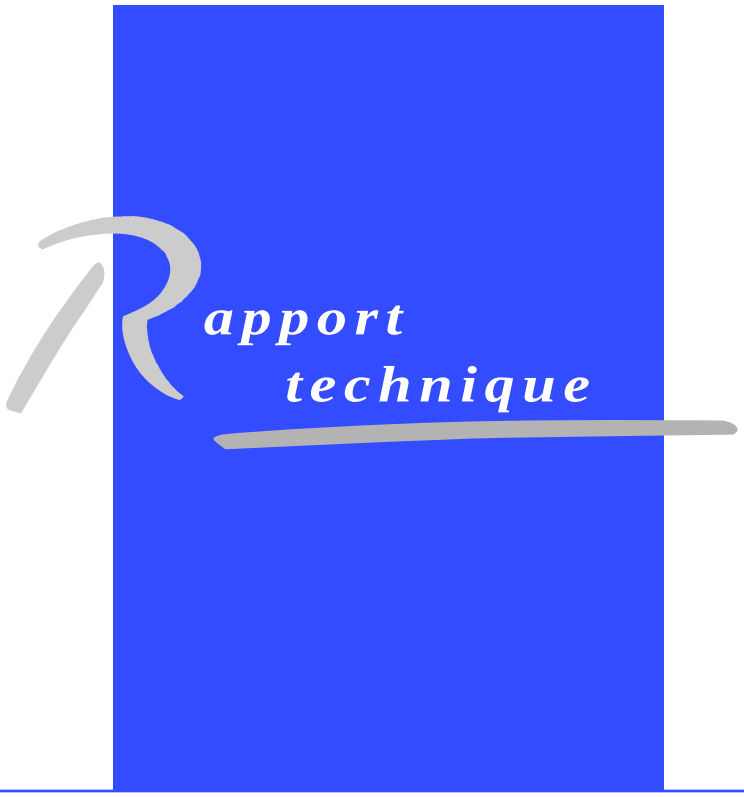
Routing and Broadcasting in Hybrid Ad Hoc Networks

François Ingelrest — David Simplot-Ryl — Ivan Stojmenović

N° 0291

Février 2004

THÈME 1



ISSN 0249-0803

Routing and Broadcasting in Hybrid Ad Hoc Networks

François Ingelrest* , David Simplot-Ryl* , Ivan Stojmenović†

Thème 1 — Réseaux et systèmes
Projet POPS

Rapport technique n° 0291 — Février 2004 — 14 pages

Abstract: Hybrid ad hoc networks consist of two kinds of nodes, regular nodes and nodes with additional capabilities. For example, multi-hop cellular and wireless Internet networks consist of static or mobile nodes and access points to a fixed infrastructure. Each node may access fixed infrastructure either directly or via other nodes in multi-hop fashion. Another example is heterogeneous sensor networks, which consists of regular tiny sensors, and special nodes capable of communicating between themselves and to monitoring station using their own backbone network. In this paper, we propose some protocols for broadcasting and routing in hybrid ad hoc networks. Hybrid blind flooding uses backbone of access nodes to spread the message, otherwise blind flooding is applied. Component neighbor elimination based flooding applies neighbor elimination based broadcasting separately within each component, consisting of all nodes with the same closest access point. In adaptive flooding, each node additionally estimates whether each of its neighbor from a different component already received the packet via its own access point in the neighbor elimination process. Multipoint relaying, and dominating set based broadcasting are generalized from existing ad hoc network protocols, utilizing the capabilities of access points. These broadcasting protocols can be applied for route discovery in proactive or reactive routing protocols for hybrid ad hoc networks. Hybrid routing protocol for hybrid ad hoc networks applies proactive routing to maintain the link to the closest access point, and reactive routing to find route between two ad hoc nodes. Access points cooperate to reduce the hop count of later route discovery.

Key-words: Hybrid Ad Hoc Networks, Energy-Efficient Protocols, Broadcasting, Routing, Multi-hop Cellular Networks, Wireless Internet.

* IRCICA/LIFL, Univ. Lille 1, INRIA futurs, France. Email: {Francois.Ingelrest, David.Simplot}@lifl.fr
† Computer Science, SITE, University of Ottawa, Ontario K1N 6N5, Canada. Email: ivan@site.uottawa.ca

Unité de recherche INRIA Futurs
Parc Club Orsay Université, ZAC des Vignes,
4, rue Jacques Monod, 91893 ORSAY Cedex (France)
Téléphone : +33 1 72 92 59 00 —Télécopie : +33 1 72 92 59 ??

Routage et diffusion d'informations dans les réseaux ad hoc hybrides

Résumé : Les réseaux ad hoc hybrides sont composés de deux types de noeuds: les noeuds ordinaires et ceux dotés de possibilités supplémentaires. Par exemple, les réseaux cellulaires multi-sauts avec accès à Internet sans fils sont composés de noeuds statiques ou mobiles et de points d'accès à une infrastructure fixe. Chaque noeud peut accéder à cette infrastructure soit directement soit en multi-sauts en passant par d'autres noeuds. Les réseaux de capteurs hétérogènes en sont un autre exemple. Ils sont composés de petits capteurs ordinaires et de noeuds spéciaux capables de communiquer entre eux et avec les stations de surveillance grâce à leur propre infrastructure de réseau. Dans cet article, nous proposons quelques protocoles pour la diffusion d'informations et le routage dans les réseaux ad hoc hybrides. L'inondation aveugle hybride utilise l'infrastructure des points d'accès pour diffuser le message si cela est possible, avec l'inondation aveugle classique dans les autres cas. La diffusion avec élimination de voisins par composantes applique le principe de l'élimination de voisins de manière séparée dans chacune des composantes, formées par tous les noeuds ayant le même point d'accès le plus proche. Dans l'inondation adaptative, chaque noeud estime en plus si ses voisins appartenant à une composante différente ont déjà reçu le message ou non par leur propre point d'accès dans le processus d'élimination de voisins. Le protocole de relais multipoints, ainsi que celui à base d'ensembles dominants sont généralisés à partir de leur version pour réseaux ad hoc, afin d'utiliser les capacités des points d'accès. Ces protocoles de diffusion peuvent être appliqués pour la découverte de routes dans des protocoles réactifs ou proactifs. Le protocole de routage hybride pour réseaux ad hoc hybrides utilise un routage proactif pour maintenir un lien vers leur point d'accès le plus proche, alors qu'un routage réactif est utilisé pour la découverte de routes entre deux noeuds en mode ad hoc. Les points d'accès y participent afin de réduire le nombre de sauts dans les routes découvertes.

Mots-clés : Réseaux ad hoc hybrides, Protocoles économiques, Diffusion d'informations, Routage, Réseaux cellulaires multi-sauts, Internet sans fils.

1 Introduction

In the past few years, the networking technology has advanced very rapidly. Internet access is a standard commodity, and most companies use local area networks to forward information between employees. Fiber optics deployment allowed high speed Internet access for personal use. The next step in technological development is to provide high quality Internet access to nomadic users, who want to check their mails or keep in touch with their office, using portable devices like cell phones, laptops or *PDA*'s (*Personal Digital Assistant*). *WLAN*'s (*Wireless LAN*) have emerged to fill this growing demand, with the *WiFi* (*Wireless Fidelity*) technology, which provides such an access to a user which is in the physical neighborhood of an access point. These access points are being deployed at densely populated stations such as airports. Despite its advantages, this technology is still very restrictive, as users have to be in the communicating range of an access point to use it. This means that a huge number of access points need to be installed to have a seamless wireless network available.

To allow greater mobility, and to reduce the impact of collisions with multiple users attached to the same access point, multi-hop access mode is being considered. Instead of direct communication with access point, it may be beneficial, in terms of energy efficiency, extended coverage, and bandwidth capacity, to contact access point via other users in multi-hop fashion. Similar scenario also exists with cellular networks in areas of high user populations, such as stadium during events. Multi-hop cellular networks are being considered as a viable alternative to direct access from mobile phone to public phone network in such scenarios.

Wireless ad hoc networks are being considered to provide multi-hop communication between peers. They are formed by a set of hosts that operate in a self-organized and decentralized manner, forming a dynamic autonomous network without relying on any fixed infrastructure. Communications take place over a wireless channel, where each host has the ability to communicate directly with any other one in its physical neighborhood, which is determined by a communicating range. These networks have multiple applications in areas where wired infrastructure may be unavailable, such as battlefields or rescue areas.

These two technologies (pure ad hoc networks, fixed infrastructure) can be combined into one to better satisfy the user needs. By using ad hoc communicating mode, fewer access points are needed to cover a 'crowded' area. The access points themselves may participate in ad hoc communication in addition to providing access to a fixed infrastructure. For instance, some nodes in a network (possibly even mobile) could be equipped with, say, satellite access for communication among themselves and for Internet access.

Fig. 1 illustrates how hybrid networks can be formed to replace existing single-hop access. Case (a) shows a wireless network that relies on a fixed infrastructure. To cover the whole area in this mode, two access points are needed. With the use of ad hoc communicating mode, illustrated in case (b), it is possible to use only one access point. Users that are relatively far from an access point may still access it, using other mobile users as relays. Such networks are referred to as being *Hybrid Ad Hoc Networks*. Examples of such networks include multi-hop cellular and wireless Internet access networks. In addition to having access to a fixed infrastructure, hybrid ad hoc networks may also provide communication between network nodes. For instance, friends may look for each other at a stadium.

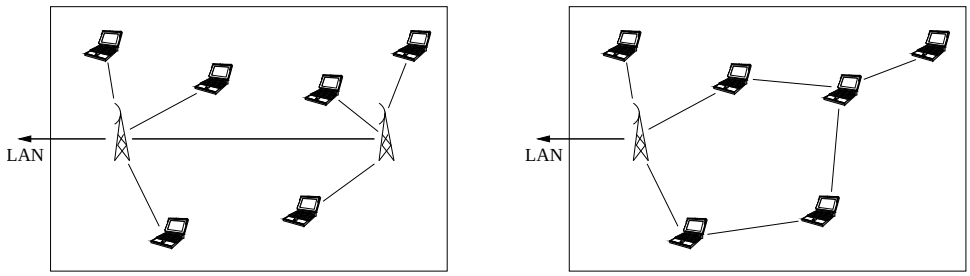


Figure 1: From single-hop access to multihop hybrid ad hoc network.

The communication may use only ad hoc network nodes, or may, in addition, involve one or two access nodes. Access nodes have some advantages over mobile nodes. They have an 'unlimited' amount of energy, and are therefore reliable node for receiving and transmitting messages. They can have same transmission range as mobile nodes, to provide symmetric communication, or could have increased transmission range for one way message transmissions. This article is mainly interested in the first case, with access nodes and mobile nodes using the same transmission ranges, assuming that all messages need to be acknowledged for reliability.

Our context of hybrid ad hoc networks is also applicable to heterogeneous sensor networks, considered by Intel for practical applications. In addition to regular tiny sensors, bandwidth and energy constrained, it contains some 'supernodes' which have much higher bandwidth and energy (possibly even no energy limitations), and which create a high bandwidth backbone for communication between themselves and connection to the monitoring station. We assume here that these 'supernodes' serve as access points to tiny sensors, and that the communication cost between them is negligible compared to the cost of communicating between regular sensors. With such assumption made, the heterogeneous sensor networks become special case of hybrid ad hoc networks, considered here as a general network model.

The goal of this paper is to consider some basic data communication problems of hybrid ad hoc networks, such as broadcasting or routing, and to propose some techniques adapted to this kind of networks. Indeed, these tasks must be performed by taking advantage of the presence of access points, and as a consequence existing algorithms for ad hoc networks must be adjusted. The organization of this article is as follows. We first define a terminology for hybrid networks in Sec. 2 and present literature review in Sec. 3. We then propose some protocols for broadcasting in Sec. 4 and for routing in Sec. 5. We finally give a brief conclusion and ideas for future works in Sec. 6.

2 Preliminaries

We represent a wireless ad hoc network by a graph $G = (V, E)$ where V is the set of vertices (mobiles or access points) and $E \subseteq V^2$ the set of edges between these vertices. An edge exists between two nodes if they are able to communicate to each other, that is two nodes u and v can communicate if they are in the communicating radius of each other. If all nodes have the same range R, the set E is then defined as:

$$E = \{(u, v) \in V^2 \mid u \neq v \wedge d(u, v) \leq R\},$$

$d(u, v)$ being the Euclidean distance between u and v. We also define the neighborhood set $N(u)$ of the vertex u as

$$N(u) = \{v \mid (u, v) \in E\}.$$

In this paper, we consider hybrid networks, which are formed by mobiles and fixed access points, denoted by P_i. Depending on their position, mobiles can be either directly connected to an access point, or constrained to use ad hoc mode if they are too distant. We assume that access points are mutually connected by a fast high bandwidth backbone network. It is reasonable to assume that access nodes are able to emit radio messages with a radius pR, p being a constant multiplier ≥ 1. A radio message emitted by an access point P_i will be received by every mobile u such that

$$d(P_i, u) \leq pR,$$

$d(P_i, u)$ being the Euclidean distance function. We use in this paper the assumption that $p = 1$, so that access points and mobiles have the same transmission radius.

We denote by $hc(u, v)$ the distance in hops between nodes u and v, which is simply the number of edges a message has to cross between these two nodes. We also denote by $AP(u)$ the closest access point to the mobile u, in term of hops. If several access points are at the same distance from the node, then the *identifier* (id) of access points is used as a tie breaker, that is the one with the smallest id is chosen.

For the sake of simplicity, we denote by $hc(u)$ the distance in hops between u and its nearest access point:

$$hc(u) = hc(u, AP(u)).$$

The set of mobiles that are attached to an access point P_i is denoted by $AN(P_i)$:

$$AN(P_i) = \{u \mid AP(u) = P_i\}.$$

We suppose that each node u regularly emits special short messages named *HELLO* messages, containing its id, denoted by $id(u)$, and the value of $AP(u)$ and $hc(u)$. We suppose that a node sets this value to $X+1$, with X the minimum value of $hc(v)$ it received, where v is any of its neighbors. If access points send their *HELLO* messages with a distance

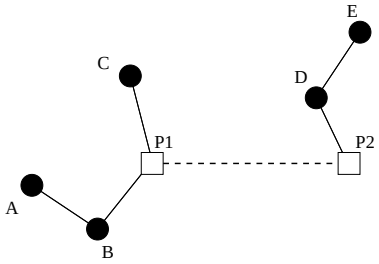


Figure 2: Example of an hybrid network with two access points.

of 0, each node is able to recursively determine its distance to the nearest access point. This process can be avoided for some protocols that do not request nodes to have information about their closest access point, like the blind flooding (see Sec. 4.1).

Fig. 2 shows an example of such an hybrid network. Squares P_1 and P_2 are access points, forming a wired network, while every other nodes (circles) are simple mobiles. In this example, we have $AP(A) = P_1$ while $AP(D) = P_2$, $AN(P_1) = \{A, B, C\}$ and $AN(P_2) = \{D, E\}$.

3 Literature review

3.1 Broadcasting

The broadcasting is defined to be a one-to-all communication, that is a mobile user sends a message that should be received by all other users in the network (provided they are connected). For further reading, an extensive review of energy-efficient broadcasting protocols for pure ad hoc networks can be found in [3].

The most basic broadcasting protocol is known as the *blind flooding*, in which a source node transmits the message to all its neighbors, and then each node that receives it for the first time re-emits it. Assuming an ideal *MAC* layer, this protocol is reliable, that is, every node in the network will receive at least once the message. However, because of its simplicity, this protocol leads to a lot of duplicated packets and thus to a huge waste in energy consumption.

A more intelligent protocol, named *Neighbor Elimination Scheme* (*NES*) has been independently proposed in [9, 7]. Its principle is as follows. Each node that receives the message for the first time does not retransmit it immediately, but waits for a given duration, which can be computed or randomly generated. Then, the node starts monitoring its neighborhood and after each received copy of the broadcast message, it eliminates from its rebroadcast list neighbors that are assumed to have correctly received it. If the list becomes empty before the node decides to relay the message, the re-emission is canceled. This protocol allows some energy savings by canceling redundant emissions, while still insuring an entire coverage of the network.

Another category of protocols is based on the computation of a connected dominating set S. A set is a dominating one if each node in the graph is either in S or a neighbor of a node in S. The broadcasting step, in its simplest variant, can be described as follows. When a node receives a broadcast message for the first time, it drops it if it is not in the considered connected dominating set, or retransmits it otherwise [9]. Nodes ignore subsequent receptions of the same message. When neighbor elimination scheme is applied, some transmissions may be avoided. A node which is in the dominating set, but observes that all its neighbors have already received the same message, can also drop the packet without retransmitting it.

Connected dominating sets may be defined in several ways. A localized algorithm that computes such a set, named "Generalized Self-Pruning Rule", can be found in [1]. In this method, each node u must be assigned a key denoted by $key(u)$, the key used in [1] being equal to $id(u)$. First, each node checks if it is an intermediate node, meaning that it has at least two neighbors which are not directly connected. Then each intermediate node u constructs a subgraph G of its neighbors with higher keys. If G is empty or disconnected then u is in the dominating set. If G is connected but there exists a neighbor of u which is not neighbor of any node from G then u is in the dominating set. Otherwise u is covered and is not in the dominating set. In this source-independent protocol, all broadcasting tasks are always supported by the same nodes. This allows the rest of nodes to be placed in sleeping mode without affecting the network operation.

If all nodes remain active, to better balance the energy consumption, some source-dependent protocols can be used. In this category, the Multipoint Relay protocol (*MPR*) was proposed by Qayyum *et al.* [8]. A node uses a greedy heuristics to compute an optimal selection of its direct neighbors to act as relays, in order to reach every of its two-hops neighbors. The node forwards this selection with the broadcast packet, and only selected nodes relay it. When neighbor elimination is added to the scheme, it works as follows. Each node receiving the message for the first time will check if it is designated as a relay node by the sender. It then eliminates all neighbors for which it knows have already received the message. A set of one-hop neighboring relay nodes is then selected to cover all two-hops neighbors as follows. Repeatedly, neighbor that covers the maximal number of uncovered neighbors is selected as relay, and covered nodes are eliminated from the list of two-hops neighbors still not covered.

3.2 Routing

When two nodes want to communicate to each other, two cases can occur: either they are neighbors, in which case they can communicate directly, or they are too distant, in which case messages must be routed. Routing is the problem of sending a packet from a source node to a destination one. A simple solution to this problem would be to broadcast the messages to the whole network. However, such a solution uses huge network capacity and leads to network congestion after only few such tasks. For a particular communication, a path must be therefore found to utilize only nodes needed for forwarding the packets.

The Dynamic Source Routing (*DSR*) is an *IETF* protocol [5], considered as possible standard for ad hoc network routing, that uses the broadcasting process to find a route between two nodes. When a host wants to find a route to another one, it initiates a broadcast containing the *id* of the searched host. Each node that receives this message inserts its *id* in the packet, and possibly some other control overhead (depending on particular variant of the considered protocol), and will retransmit it. Since the broadcast reaches every connected node in the network, the destination will receive it and will be able to reply to the source by following the chain of nodes traversed by the packet in the reverse order. When the reply is received, a communication route has been established between the two nodes.

While reactive protocols, like *DSR*, create routes only when they are needed, a proactive one creates and maintains routes before their use. To do so, each host maintains routes to other ones in the network by exchanging routing tables between neighbors. These routing protocols can be also used in hybrid networks. Although this proactive algorithms allow a source node to immediately have a route to a destination, they may require a large amount of data for their maintenance and therefore cause huge communication overhead. Some efficient proactive protocols have been proposed for pure ad hoc networks, such as Optimized Link State Routing (*OLSR*) [4], in which *MPR* is used for route maintenance.

We identified only two routing protocols for hybrid wireless networks in the literature. Li *et al.* proposed in [6] a system that connects public service buses to form a wireless network. Some stationary gateways have to be installed along the roads for users to be able to access to the Internet. Communications between buses and gateways can be done directly or in ad hoc mode, depending on the distance between them. In ad hoc mode, buses serve as relays for other ones not directly connected. The routing task is done by a top level router, which knows the closest gateway for each bus using any proactive or reactive method. When a message has to be routed, the closest gateway forwards it to the top level router, which redirects it to the destination gateway or to the Internet, as needed.

In [2], Fujiwara *et al.* proposed a mechanism that allows nodes to maintain their routes to the base station via multi-hopping if needed. If a direct link between any node and its base station is broken, the node starts monitoring communications in its neighborhood to find a node that is still connected to the base station, either directly or by multi-hopping. When the node finds a connected neighbor, which should be one hop nearer, it marks it as its 'router' and sends to it the packets that must be sent to the access point. This allows nodes to always be able to connect to their base station.

4 Broadcasting

We propose here several broadcasting protocols for hybrid ad hoc networks. These protocols are either new or generalizations of existing protocols for pure ad hoc networks described in Sec. 3.1.

4.1 Hybrid Blind Flooding

This protocol is a very simple extension of existing blind flooding protocol for pure ad hoc networks. In this protocol, each node, receiving packet for the first time, will retransmit it. Subsequent copies of the same packet are ignored. If the node that received packet (or a source node) is an access point, then all other access points receive the packet via their backbone network. Therefore in the next step all access points may retransmit the message.

4.2 Component Neighbor Elimination Based Flooding

This protocol is based on an observation that transmissions from mobiles to other ones directly connected to an access point are a waste of energy. Indeed, the mobile could have received the message from the access point, which would have been done 'for free' (we do not take into account energy spent by access points).

To prevent these useless transmissions and to allow access points to be the first ones to reach their neighborhood, we divide the network into components, one for each access point. Each component $C(P_i)$ is defined by:

$$C(P_i) = \{P_i \cup AN(P_i)\}.$$

We can notice that these components are connected, since there exists a path between any node in $AN(P_i)$ and P_i. To further limit energy consumption, we use a neighbor elimination scheme.

To limit the propagation inside each component, we suppose that there exists a field named P_{msg} in the broadcast packet, that defines which component is going to be flooded, *i.e.* only nodes within the component $C(P_{msg})$ relay the message. When the message is transmitted for the first time by a node s, the value of P_{msg} is set to $AP(s)$, in order to flood the component $C(AP(s))$. A node u that receives a message with $P(u) \neq P_{msg}$ does not relay it. Otherwise, if it is the first reception, it enters a *NES*, monitors its neighborhood and relays the packet at the end of the timeout only if there exists uncovered neighbors in $P(u)$. When the access point $AP(s)$ receives the message, it relays it to all other access points. Depending on the structure of the network of access points, this can be done by direct forwarding to each of them, or by applying a corresponding broadcast protocol among access points. When an access point P_i receives the message for the first time, it changes the value of P_{msg} to its own *id* before rebroadcasting it via the radio interface to all nodes in its component.

4.3 Adaptive Flooding

The main drawback of the component neighbor elimination based flooding is its increased latency, which is the elapsed time between the start of the broadcast and its end. Indeed, some nodes which could have received the message earlier from a close neighbor in other component are ignored, because they have different respective access points. The *adaptive flooding* is designed to minimize the latency of the broadcast.

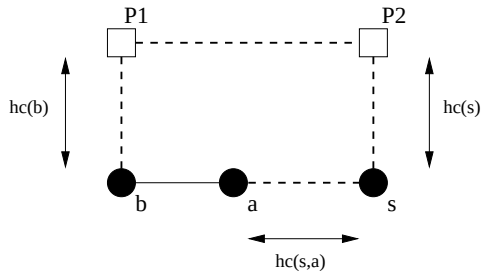


Figure 3: Illustration of the distances for adaptive flooding.

For a given node a, there are two ways to receive the message:

- in "ad hoc mode", from the source node s, or other node (in the same or different component as s), without passing through any access point,
- in "access point mode", from the node s to $AP(s)$, from $AP(s)$ to $AP(a)$ and from $AP(a)$ to the node a. We assume that the cost of the communication (in terms of duration) between $AP(s)$ and $AP(a)$ is equal to zero.

This protocol selects the shorter path between these two modes to reduce the overall latency. When a node a receives from a node p a broadcast message initiated by a node s, two cases can happen:

1. The message has not crossed an access point. The node a decides to forward the message if there exists a node b which belongs to $N(a) \setminus N(p)$ such that $hc(s,a) + 1 < hc(s) + hc(b)$. In this case, $hc(s,a)$ can be approximated by the number of links the message has crossed from s to a and $hc(s)$ should have been written in the packet by s. These distances are illustrated in Fig. 3. Note that the message may cross several components in this process.
2. The message has crossed an access point. Each node relays the message if there exists a neighbor, in the same component, that would benefit from this retransmission. That is, the corresponding access point of the component is treated as the message source, neighbors from other components are ignored, and neighbor elimination based flooding is applied within the component. Note that some nodes in the same component could have received the same message by applying the first 'non-crossing access point' mode, and these nodes do not participate in this mode (except in cases when they did not retransmit the message, and neighbors, not knowing about their reception, could transmit because of them).

4.4 Multipoint Relay Broadcasting Protocol

This protocol is very efficient in terms of energy savings, and can be easily generalized to hybrid networks. Mobile nodes should be used as relays only if they are needed besides access points. When considering which neighbors should relay, access points (if any in the neighborhood) should be first added to the list of relays and then, if there remains some uncovered two-hops neighbors, an optimal selection of remaining neighboring relay nodes should be computed.

If we assume that mobiles do not have components information, this protocol can be applied without any further modification. When an access point receives the message, it simply has to send it to the other access points to speed up the broadcasting process. However, if mobiles are aware about their component membership, and the hop count distances of the source, one-hop or even two-hops neighbors to their corresponding access points, some transmissions could be avoided. For instance, two-hops neighbors a for which $hc(s,a) > hc(s) + hc(a)$ do not need to be covered (note that current node adds two hops to its own distance to s to its estimate for $hc(s,a)$ which may not be a correct value).

4.5 Dominating Sets Based Broadcasting Protocol

The generalized self-pruning rule, as described in Sec. 3.1, is very flexible since the key can be composed by any collection of values, while still guaranteeing the construction of a connected dominating set. To adapt it to hybrid networks, we replace the *id* by two values, so that the key $key(u)$ of a node u is defined by:

$$key(u) = \{E_u, id(u)\}, \tag{1}$$

E_u being the energy level of u. The comparison between two keys is made using their primary keys, and if they are equal then the comparison is made using the secondary key. If we consider that access points have an 'infinite' amount of energy, they will always be selected as dominant and thus will be part of the broadcasting process.

Fig. 4 shows an example of the application of such key definition, square 0 being an access point and circles being mobiles. Case (a) is the result of the generalized rule applied with *id*'s of nodes used as keys, while in case (b), *id*'s have been replaced by the key given in Eq. 1. Access point 0 has been selected in the dominating set, and as a result nodes 2, 3 and 4 are now covered (not in dominating set), so that they will not spend their energy for the broadcast process.

5 Routing

5.1 Adaptation of existing protocols

The simplest way to adapt routing protocols like *DSR* or *OLSR* to hybrid networks is obviously to replace the broadcasting protocol by its adapted version as described in previous sections.

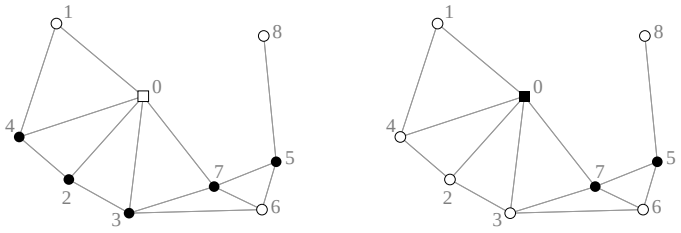


Figure 4: Generalized self-pruning rule applied to hybrid networks.

For example, the broadcasting step of *DSR* could use a variety of protocols, depending on the taken assumptions. If we assume that nodes do not have any information about their closest access point, one can use the blind flooding, as defined in the original version of *DSR*. However if we remove this assumption, some more intelligent protocols can be used. For example, by using a dominating sets based protocol, the number of retransmissions will be reduced. The version adapted to hybrid networks gives a top priority to access points, so that they will be used whenever it is possible for routing in *DSR*, saving energy for mobile nodes. The adaptive flooding could also be used, which would led to the discovery of the shortest paths, as the protocol always chooses the shortest one to reach every node.

Similar discussion is valid for *OLSR*, which can take advantage of the presence of access points if *MPR* is modified appropriately, as described in previous section.

5.2 Hybrid Routing for Hybrid Ad Hoc Networks

This protocol allows mobiles to communicate to each other by using the faster mode between infrastructure or ad hoc communicating mode. It is a hybrid routing protocol since it combines proactive and reactive approaches. Proactive routing is used to maintain links of each ad hoc node to its access point, while reactive routing is used to find routes between two adhoc nodes. We assume that nodes know the component memberships and that each access point P_i knows the mobiles that are in $AN(P_i)$ and the hop distance to each of them. For example, the Fujiwara's protocol [2] could be used to achieve this. When a node u wants to communicate with a node v, two modes can be used:

- The infrastructure mode. The node u sends the packets to $AP(u)$, which forwards them to $AP(v)$. Access points can periodically exchange their routing tables to determine which one has to be contacted depending on the packet that has to be routed. Finally, $AP(v)$ will forward packets to v.

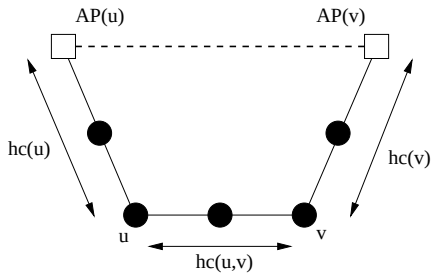


Figure 5: Ad hoc communicating mode can be faster than infrastructure mode.

- The ad hoc mode. The node u sends the packets 'directly' to v, by using other mobiles as relays.

As illustrated by Fig. 5, the ad hoc communicating mode can sometimes be faster (the path is shorter) and should be used to speed up the routing process. To determine which mode to use, the node u first asks the value of $hc(v)$ to $AP(u)$. If $AP(u)$ does not have this information, it requests it from other access points in the wired network. When u retrieves $hc(v)$, it launches a broadcast with a Time-To-Live (TTL) equal to $hc(A) + hc(B) - 1$ to find a route in pure ad hoc mode (by using *DSR* for example). If v is not found by using this broadcast, it means that the path between them in ad hoc mode is longer than the one in infrastructure mode (*i.e.* $hc(u, v) > hc(u) + hc(v)$). In this case, the infrastructure mode will simply be used. By using this protocol, any two nodes can communicate to each other by knowing their routes and distances to access points.

It can be noticed that packets can be re-routed by any node in infrastructure mode if needed. Indeed, if a packet that has to be routed via a certain path arrives at a node which knows that this route is no longer available, it can re-route the packet by using its own path to the access point. The latter and the source node will then update their routing tables.

6 Conclusion

In this paper, we have considered hybrid networks, which are composed of mobiles ad hoc network and access points, in which the ad hoc communicating mode is available to increase the flexibility and mobility of users. A terminology was introduced that allows one to easily describe such a network. We also presented several algorithms for basic data communication tasks in a network, such as broadcasting and routing. These algorithms are adapted from ad hoc networks to hybrid networks, to take advantage of access point as much as possible.

In our future work, we want to further improve some of these protocols and to design some experiments to obtain their respective performances, which could allow a fair comparison between them. We want to study broadcast protocols involving topology management with radius adjustment in hybrid networks. Finally, some assumptions can also be removed and

their consequences studied. A particular example is the case in which access points have a a constant factor p times greater larger transmission radius than the maximum radius of ad hoc mobile nodes.

References

[1] F. Dai and J. Wu. Distributed dominant pruning in ad hoc networks. In *Proceedings of the IEEE International Conference on Communications (ICC'03)*, Anchorage, AK, USA, May 2003.

[2] T. Fujiwara, N. Iida, and T. Watanabe. An ad hoc routing protocol in hybrid wireless networks for emergency communications. In *Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN'04) at IEEE International Conference on Distributed Computing Systems (ICDCS'04)*, Tokyo, Japan, March 2004.

[3] F. Ingelrest, D. Simplot-Ryl, and I. Stojmenović. *Resource Management in Wireless Networking*, chapter 17 'Energy-Efficient Broadcasting in Wireless Mobile Ad Hoc Networks'. Kluwer, 2004. To be published.

[4] P. Jacquet, P. Mühlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot. Optimized link state routing protocol for ad hoc networks. In *Proceedings of the IEEE International Multi-topic Conference (INMIC'01)*, Lahore, Pakistan, December 2001.

[5] D.B. Johnson, D.A. Maltz, and Y.-C. Hu. The dynamic source routing protocol for mobile ad hoc networks (DSR). Internet Draft, draft-ietf-manet-dsr-09.txt, April 2003. Work-in-progress.

[6] T. Li, C. K. Mien, J. L. S. Arn, and W. Seah. Mobile internet access in BAS. In *Proceedings of the International Workshop on Wireless Ad Hoc Networking (WWAN'04) at IEEE International Conference on Distributed Computing Systems (ICDCS'04)*, Tokyo, Japan, March 2004.

[7] W. Peng and X.C. Lu. On the reduction of broadcast redundancy in mobile ad hoc networks. In *ACM MobiHoc 2000*, pages 129 – 130, Boston, Massachusetts, USA, August 2000.

[8] A. Qayyum, L. Viennot, and A. Laouiti. Multipoint relaying for flooding broadcast messages in mobile wireless networks. In *Proceedings of the Hawaii International Conference on System Sciences (HICSS'02)*, January 2002.

[9] I. Stojmenović and M. Seddigh. Broadcasting algorithms in wireless networks. In *Proceedings of the International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet SSGRR*, L'Aquila, Italy, July 31-Aug. 6 2000.

Unité de recherche INRIA Futurs
Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)

Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-0803