HAL
open science

Broadcasting in Hybrid Ad Hoc Networks.

François Ingelrest, David Simplot-Ryl, Ivan Stojmenovic

To cite this version:

François Ingelrest, David Simplot-Ryl, Ivan Stojmenovic. Broadcasting in Hybrid Ad Hoc Networks.. The Second Annual Conference on Wireless On demand Network Systems and Services (WONS 2005)., Jan 2005, St Moritz, Switzerland. inria-00000032

HAL Id: inria-00000032

https://inria.hal.science/inria-00000032

Submitted on 17 May 2005

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Broadcasting in Hybrid Ad Hoc Networks

François Ingelrest and David Simplot-Ryl
IRCICA/LIFL, INRIA futurs
University of Lille 1
Villeneuve d'Ascq, France
Email: {ingelres, simplot}@lifl.fr

Ivan Stojmenović
Computer Science, SITE
University of Ottawa
Ontario K1N 6N5, Canada
Email: ivan@site.uottawa.ca

Abstract

In this paper, we consider hybrid ad hoc networks, which are composed of two kinds of nodes, regular ones and nodes with additional capabilities. For example, multi-hop cellular and wireless Internet networks consist of static or mobile nodes, and fixed access points which provide an access to an infrastructure. In such a network, each node may use direct or multihop link to connect to an access point, allowing a greater mobility. The goal of this paper is to provide protocols for broadcasting data in such an environment, by taking advantage of the presence of access points to optimize the broadcast, either from an energy consumption or from a latency point of view. We thus consider known protocols for pure ad hoc networks and adapt them to hybrid ad hoc networks. These protocols are the Blind Flooding, the Neighbor Elimination Scheme, the Multipoint Relay protocol and the generalized Self-Pruning Rule (algorithm that elects some dominant nodes to relay messages). We give some experimental data for these modified protocols to compare them to their original version, so that we are able to emphasize the gain obtained thanks to our proposed modifications.

1 Introduction

In the past few years, the networking technology has advanced very rapidly. Internet access is a standard commodity, and most companies use LANs (*Local Area Network*) 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 PDAs (*Personal Digital Assistant*). WLANs (*Wireless LAN*) have emerged to fill this growing demand, with the WiFi (*Wireless Fidelity*) technology, which provides such an access to users which are in the physical neighborhood of an access point (AP in short). These access points are being deployed at densely populated stations such as airports or train stations. Despite its advantages, this technology is still very restrictive, as users have to be in the communicating range of an AP to use it. This means that a large number of them need to be installed to have a seamless wireless network available.

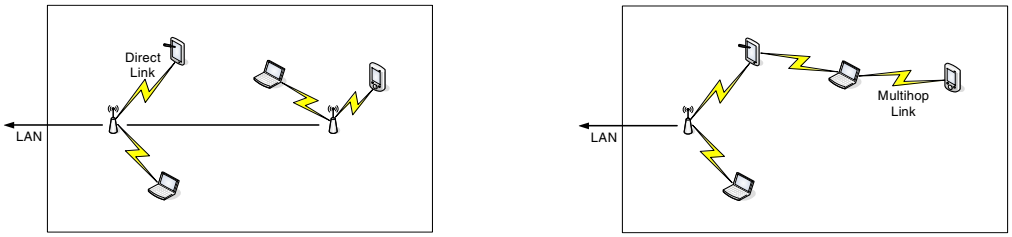
To allow greater mobility, and to reduce the impact of collisions with multiple users attached to the same AP, multi-hop access mode is being considered. Instead of directly communicating with APs, it may be beneficial, in terms of energy efficiency, extended coverage, and bandwidth capacity, to connect to them via other users in a multi-hop fashion. Similar scenario also exists with cellular networks in areas of high user populations, such as a 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.

At the same time, wireless ad hoc networks are being studied 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 the 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 given 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.

Proceedings of the Second Annual Conference on Wireless On-demand Network Systems and Services (WONS'05)
0-7695-2290-0/05 $ 20.00 IEEE

IEEE COMPUTER SOCIETY



(a) (b)

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

Figure 1 illustrates how hybrid networks can be formed to replace existing single hop access. Case (a) shows a wireless network that entirely 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 by case (b), it is possible to use only one access point. Users that are relatively far from an AP may still access to 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. The communication may use only ad hoc network nodes, or may, in addition, involve one or two access points. The latter have some advantages over mobile nodes. They have an 'unlimited' amount of energy, and are therefore reliable nodes for receiving and transmitting messages. They can have the same transmission range as mobile nodes, to provide symmetrical communication, or could have increased transmission range for one way message transmissions. This article is mainly interested in the first case, with access points and mobile nodes using the same transmission range.

Our context of hybrid ad hoc networks is also applicable to heterogeneous sensor networks, considered by Intel for practical applications [4]. 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, 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 the problem of broadcasting in hybrid ad hoc networks, and to propose some techniques adapted to this kind of networks. Indeed, a task like broadcasting 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 paper is as follows. We first define a terminology for hybrid ad hoc networks in Sec. 2 and present literature review in Sec. 3. We then propose some broadcasting protocols in Sec. 4 and some experimental results for these protocols in Sec. 5. We finally give a brief conclusion and direction for future work 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 in this paper) 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. Two nodes u and v can communicate together if they are in the communicating radius of each other. If all nodes have the same communication 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 nodes u and v. We also define the neighborhood set $N(u)$ of the vertex u as

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

The density is defined to be the number of nodes in a communication area (circle of radius R).

In this paper, we consider hybrid networks, which are formed by mobiles and fixed access points, the latter being 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

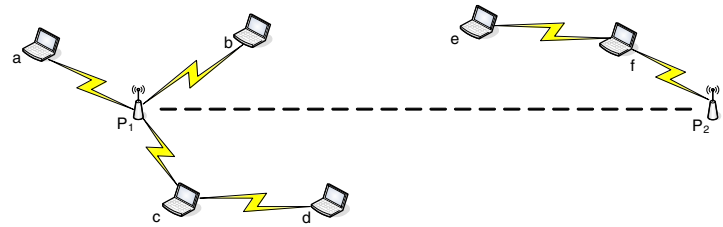


Figure 2. Example of an hybrid network with two access points.

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

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

We use in this paper the assumption that $p = 1$, so that access points and mobiles have the same transmission radius.

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

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

$$\mathrm{hc}(u) = \mathrm{hc}(u, \mathrm{AP}(u)).$$

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

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

We suppose that each node u regularly emits special short messages named HELLO messages, containing its id, denoted by $\mathrm{id}(u)$, and the value of $\mathrm{AP}(u)$ and $\mathrm{hc}(u)$. We suppose that a node sets this value to $X + 1$, with X the minimum value of $\mathrm{hc}(v)$ it received, where v is any of its neighbors. If access points send their HELLO messages with a distance 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 (see Sec. 4).

Figure 2 shows an example of such an hybrid network. Nodes P_1 and P_2 are access points, forming a wired network, while $\{a, b, c, d, e, f\}$ are simple mobiles. In this example, we have $\mathrm{AP}(a) = P_1$ while $\mathrm{AP}(e) = P_2$, $\mathrm{AN}(P_1) = \{a, b, c, d\}$ and $\mathrm{AN}(P_2) = \{e, f\}$.

3 Literature review

The broadcasting task 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 that the latter is 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 its neighborhood. Recursively, 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 [2, 5]. 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 same 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 ensuring an entire coverage of the network. However, as a counterpart, the latency is increased (the time elapsed between the first emission and the last reception).

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 [2]. 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 $\mathrm{key}(u)$, the key used in [1] being equal to $\mathrm{id}(u)$ (other metrics can however be used [7]). 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_h of its neighbors with higher keys. If G_h is empty or disconnected then u is in the dominating set. If G_h is connected but there exists a neighbor of u which is not a neighbor of any node from G_h then u is in the dominating set. Otherwise u is covered and is not in the dominating set. In this protocol, all broadcasting tasks are always supported by the same nodes, this is referenced to as source-independent protocol. 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. [6]. A node that wants to emit a broadcast message computes a 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. Each node receiving the message for the first time checks if it is designated as a relay node by the sender, and if it is the case, the message is forwarded. As computing an optimal selection of neighbors is NP-complete, MPR uses a greedy heuristics: Repeatedly, the neighbor that covers the maximal number of uncovered two-hops neighbors is selected as relay, and covered nodes are eliminated from the list of two-hops neighbors still not covered. This is done until this list becomes empty.

4 Broadcasting Protocols for Hybrid Ad Hoc Networks

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 the previous section.

4.1 Hybrid Blind Flooding

This protocol is a straightforward extension of the existing Blind Flooding protocol for pure ad hoc networks. In this protocol, each node that receives a packet for the first time will retransmit it, while subsequent copies of the same packet are ignored. When an access point receives the packet from a mobile user for the first time, it forwards it immediately to the other access points using their backbone network. Therefore in the next step all access points may retransmit simultaneously the message. Such a behavior greatly decreases the time needed to flood the network.

4.2 Component Neighbor Elimination Scheme

This protocol is based on the 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 APs).

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:

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

We can notice that these components are connected, since by definition there exists a path between any node in $\mathrm{AN}(P_i)$ and P_i. To further limit energy consumption, we use a Neighbor Elimination Scheme (of course, access points do not perform it, they immediately relay messages with their full power of transmission). Moreover, and this is perhaps the most important point, each node entering a NES only have to monitor its neighbors that belong to its own component, thus greatly reducing the probability of rebroadcasting for borderline nodes.

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 $C(P_{\mathrm{msg}})$ relay the message. When the message is transmitted for the first time by a node s, the value of P_{msg} is set to $\mathrm{AP}(s)$, in order to flood the component $C(\mathrm{AP}(s))$. A node u that receives a message with $P(u) \neq P_{\mathrm{msg}}$ 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 $\mathrm{AP}(s)$ receives the message, it relays it to all other access points using the wired backbone network. 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 its neighbors.

IEEE COMPUTER SOCIETY

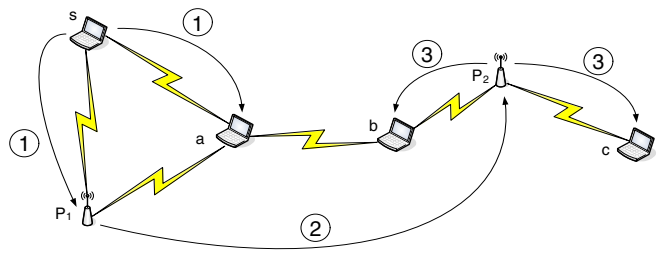


Figure 3. Example of how works the Component Neighbor Elimination Scheme.

We illustrate this protocol with Fig. 3, where s is a mobile node that launches a broadcast (1). All its neighbors (P_1 and a) receive it: P_1 sends it to P_2 using the backbone network (2), but neither P_1 (no uncovered neighbor) nor a (no uncovered neighbor in the same component, as b belongs to $\mathrm{AN}(\mathrm{P}_2)$) relays it using the radio interface. Then, P_2 sends it to b and c (3), and the broadcast is finished. With a standard NES, a would have sent the message to b, as the latter is not covered by s, and a would not have received the emission from P_2.

4.3 Adaptive Flooding

The main drawback of the Component Neighbor Elimination Scheme 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.

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 $\mathrm{AP}(s)$, from (s) to $\mathrm{AP}(a)$ and from $\mathrm{AP}(a)$ to the node a. We assume that the cost of the communication (in terms of duration) between $\mathrm{AP}(s)$ and $\mathrm{AP}(a)$ is equal to zero.

This protocol selects the shortest 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 $\mathrm{hc}(s,a) + 1 < \mathrm{hc}(s) + \mathrm{hc}(b)$. In this case, $\mathrm{hc}(s,a)$ can be approximated by the number of links the message has crossed from s to a and $\mathrm{hc}(s)$ should have been written in the packet by s. 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 Component Neighbor Elimination Scheme 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 Hybrid Multipoint Relay Protocol (MPR)

The protocol MPR is very efficient in terms of energy savings, and can be easily generalized to hybrid ad hoc 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 $\mathrm{hc}(s,a) > \mathrm{hc}(s) + \mathrm{hc}(a)$ do not need to be covered (note that current node adds two hops to its own distance

IEEE COMPUTER SOCIETY

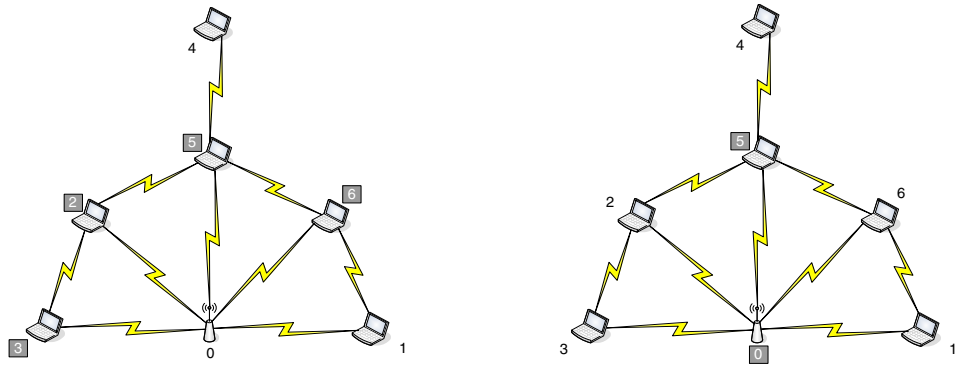


Figure 4. Generalized Self-Pruning Rule applied to hybrid networks.

to s to its estimate for $\mathrm{hc}(s, a)$ which may not be a correct value).

4.5 Dominating Sets Based Broadcasting Protocol

The generalized Self-Pruning Rule which elects dominant nodes, as described in Sec. 3, 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 $\mathrm{key}(u)$ of a node u is defined by:

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

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.

Figure 4 shows an example of the application of such key definition, node 0 being an access point while other ones are mobiles. Nodes with their id written in a square are dominant, other ones are passive. Case (a) is the result of the generalized rule applied with the id of nodes used as keys, while in case (b), id has been replaced by the key given by (1). Access point 0 has been selected in the dominating set, and as a result nodes $\{2, 3, 6\}$ are now covered (they are no longer dominant), so that they will not spend their energy for the broadcast process.

5 Experimental Results

In the simulations, we compare the proposed protocols with their 'original' version applied to the same networks. That means that they immediately 'gain' some energy thanks to the presence of access points, so that we are able to emphasize the gain obtained thanks to our modifications only.

The parameters of our simulations are the following. The network is static and is always composed of 300 nodes randomly placed in a square area whose size is computed to obtain the density of 15. The maximum communication radius R is fixed to 250 meters. The MAC layer is assumed to be ideal, that is no collision occurs when two neighbors emit simultaneously. The timeout used in the Neighbor Elimination Scheme is randomly generated. For each measure, 1000 broadcasts are launched and for each broadcast, a new network is generated. Only connected networks are kept.

To compare the different protocols, we observe the total power consumption over the network when a broadcast has occurred. For each broadcast, we compute the total energy consumption, which corresponds to the number of transmitted messages:

$$E_{\mathrm{total}} = \sum_{u \in V} E(u),$$

where $E(u)$ is defined as:

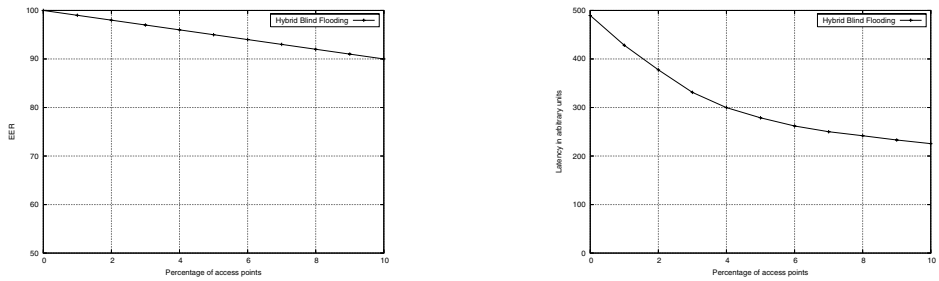
$$E(u) = \begin{cases} 1 & \text{if } u \text{ retransmits the message,} \\ 0 & \text{otherwise.} \end{cases}$$

The total energy consumption E_{total} is compared with the energy consumption that would have been spent by a Blind Flooding:

$$E_{\mathrm{flooding}} = n,$$

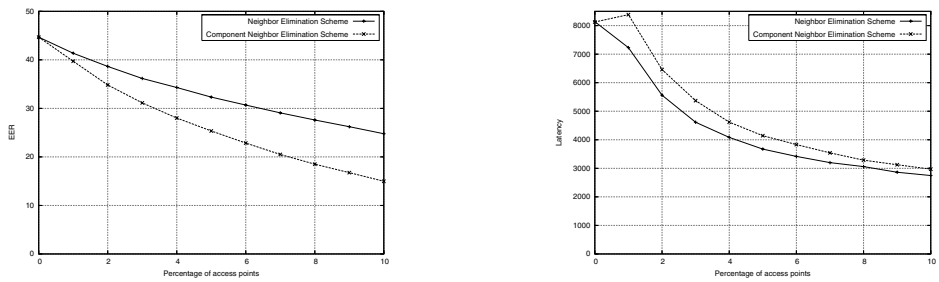
where n is the number of mobile hosts in the network.

Finally we can compute the average *Expanded Energy Ratio* (EER) which is defined by:



(a) (b)

Figure 5. Performances of hybrid blind flooding.



(a) (b)

Figure 6. Performances of the Component Neighbor Elimination Scheme.

$$\mathrm{EER} = \frac{E_{\mathrm{total}}}{E_{\mathrm{flooding}}} \times 100.$$

Thus, the lower the EER is, the lower the energy consumption is. For example, a value of 10% for a given protocol indicates that this protocol only consumes 10% of the energy that would have been spent by a simple Blind Flooding over the same network.

Considering Fig. 5, we give in (a) the energy consumption of the Hybrid Blind Flooding protocol. As expected, the value of the EER decreases linearly with the percentage of access points. If there are 10% of access points in the network, then 10% of the emissions are not taken into account. As access points immediately send messages between each other using the wired network, we logically notice in (b) a decrease in the broadcast latency as the percentage of AP increases.

Figure 6 gives the results obtained by the Component Neighbor Elimination Scheme algorithm. It can be noticed in (a) that our proposed algorithm obtains better results than the standard NES. The greater part of energy savings comes from the nodes which are at the borderline of components: when monitoring their neighborhood, they do not have to consider a big part of their neighbors (which belongs to another component). However, the drawback of this method is its increased latency as illustrated by (b). Indeed, nodes that are not taken into account (because they belong to a different component) must wait for the message to propagate between their nearest AP and them.

In Fig. 7 we give the performances of the Generalized Self-Pruning Rule. The 'standard' version uses the original definition of the key given in [1], that is, the key of a node is equal to its id. The 'hybrid' version uses the definition given in Sec. 4.5, thus access points have priority over mobile nodes. As expected, the energy consumption decreases as the percentage of AP increases.

We finally give in Fig. 8 a comparison of the performances obtained by the different protocols. Only the hybrid multipoint relay protocol needs 2-hops information, all the other ones uses only 1-hop information. As shown in (a), the Component Neighbor Elimination Scheme obtains the best performances among the others when there is at least 2% of access points in the network. Before that limit, hybrid MPR and hybrid generalized Self-Pruning Rule give nearly the same performances. From the latency point of view as shown in (b), the hybrid Blind Flooding no surprisingly obtains the best results. The latency of the Component NES decreases as the number of AP increases since the diffusion becomes less sequential when there are many AP. The latency of the Adaptive Flooding first increases since its be-

IEEE COMPUTER SOCIETY

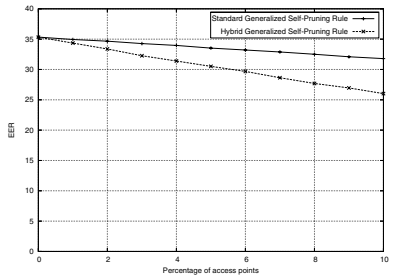
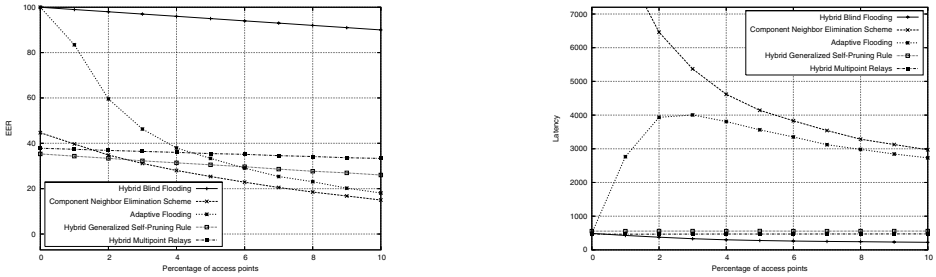


Figure 7. Performances of the modified generalized Self-Pruning Rule.



(a) (b)

Figure 8. Performances of the different schemes.

haviors is to perform a Component NES when an AP has been crossed, so the more AP there are, the more the latency increases. It becomes more or less stable when there are a sufficient number of AP since the diffusion becomes less sequential.

6 Conclusion

In this paper, we have considered hybrid ad hoc networks, which are composed of mobiles users 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 data broadcasting in a network. These algorithms are adapted from ad hoc networks to hybrid ad hoc networks, to take advantage of access point as much as possible.

In our future work, we want to further improve these protocols, for example by considering radius adjustment, which should lead to better performances. However, this brings some topology management problems which must be carefully considered. Moreover, we also want to study the case in which access points have 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, Alaska, May 2003.

[2] I. S. (Ed.) 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 2000.

[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] Intel. http://www.intel.com/research/exploratory/heterogeneous.htm.

[5] W. Peng and X. Lu. On the reduction of broadcast redundancy in mobile ad hoc networks. In *Proceedings of the ACM MobiHoc 2000*, Boston, USA, August 2000.

[6] 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)*, Big Island, Hawaii, January 2002.

[7] J. Shaikh, I.Stojmenović, and J. Wu. New metrics for dominating set based energy efficient activity scheduling in ad hoc networks. In *Proceedings of the 3rd International Workshop on Wireless Local Networks (WLN 2003)*, Bonn, Germany, 2003.