Proceedings of 5th Intl. Workshop on Mobile Multimedia Communication *MoMuc'98*, October 12-14 1998, Berlin

Wireless Multicasting in an IP Environment

Neda Nikaein, Christian Bonnet

Abstract—In a wireless network, bandwidth is a scarce resource and low power consumption is desired for mobile hosts. These constraints have not been taken into account in the multicast IP model. In this paper, we present a general framework for multicasting optimized for wireless IP systems. A general wireless IP access system has been taken as a starting reference. A specific group membership protocol has been developed for this system. The effect of mobility on multicasting has been investigated in a mobile IP environment. This multicasting scheme has been applied to the wireless IP system developed within the ACTS project Magic WAND (Wireless ATM Network Demonstrator).

Index Terms—Multicast communication, Mobility.

I. Introduction

Multicasting is the process of delivering a packet to several destinations using a single transmission. Multicast communication involves more than two users wishing to exchange information [7]. The advantage of multicast communication is its efficient use of bandwidth and network resources. The sender can transmit the data with a single transmission to all receivers. Multicast applications are becoming more and more popular. Examples of such applications include audio and video conferencing, distributed games, and computer supported collaborative work (CSCW). Hence it is important that the future wireless networks can support multicast communications.

The Internet is changing from a traditional best-effort services model to an integrated services model capable to support a variety of multimedia and real-time applications. On the other hand, the mobility features of IPv6 [4], [5], [10], [13] and mobile IP [12] make the IP protocol suitable even in mobile networks. Therefore, IP is one of the leading contenders for wireless access networks.

Originally, the ACTS Magic WAND project has been designed to provide a high speed indoor wireless ATM system with guaranteed QoS [11]. In this system, IP services are provided using LAN Emulation (LANE) [3]. However , all IP traffic is treated as best effort data. With the rapid growth of Internet and its support for mobility and QoS, the WAND project has started to specify a wireless IP access system to transmit native IP traffic. The target environment is based on the IPv6 protocol due to its potentials. The proposed concept enables full exploitation of real-time IP applications in mobile environment. The architecture of this wireless IP system can be found in [2].

The authors are with EURECOM Institute, Mobile Communication Department, BP 193, 06904 Sophia Antipolis, France. Email: {nikaein, bonnet}@eurecom.fr

IP supports multicast applications via multicast IP model. The wireless interface causes specific requirements for multicast communication which have not been taken into account in this model. This paper describes a framework for multicast communication in a wireless IP environment. We present a group membership management mechanism optimized for wireless networks. We study the effect of terminal mobility on the multicast communications in a mobile IPv6 environment. The system is able to inter-operate with multicast routing protocols existing in the backbone network. However, this paper does not treat the problem of multicast routing protocols.

The rest of the paper is organized as follows. Section II describes a generic wireless IP access network as a starting reference. Section III discusses the multicast IP model and its problems when applied to wireless networks. Section IV presents a framework for wireless multicasting. The effect of mobility on multicasting is studied in Section V. Section VI discusses the application of this multicast scheme to the WAND wireless IP architecture. Section VII concludes the paper.

II. General System Architecture

Figure 1 illustrates a generic model for a wireless IP access system. The model is composed of three components: *Mobile Terminal* (MT), *Access Point* (AP) and *Mobility Domain IP Router* (M-router).

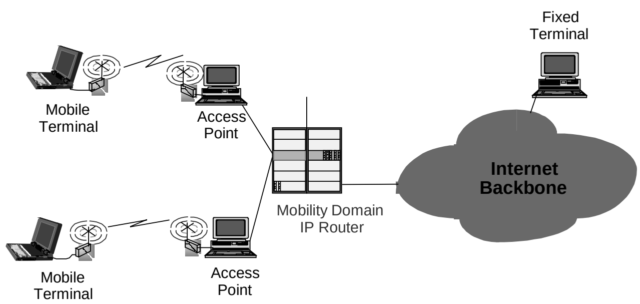

Figure 1: General system architecture.

MT is a standard IP host with a radio adapter card to access the wireless network. AP is in charge of all the radio dependent control functionality. It is the connection point of the wireless world with the wireline world. M-router manages one or more APs. It supports the interconnection of the access network to the rest of the Internet. All the APs attached to the same M-router belong to the same IP domain. The intra-domain mobility is managed by the radio link layer in APs and is completely transparent to the network layer. Terminal mobility between different IP domains is supported via IPv6 mobility functions where an MT has two IP addresses: a temporary address known as care of address and a permanent address known as home address. The care-of-address changes each time that the MT changes its point of attachment to the Internet. The home address, however, does not change. This is the address obtained by the MT in its home network. Each home network should have a router called home agent (HA) which maintains the current location of each MT registered in that network domain. The HA is able to forward the datagrams to departed MTs. The M-router provides mobility services as well as home agent functionality. The home agent can also be a separate entity.

III. MULTICAST IP MODEL

A group is a set of hosts identified by an abstract class D IP address. A source can send data to a group address without knowing the group members. Multicast IP standard uses the Internet Group Management Protocol (IGMP) [6] in order to keep track of group members in a local network. For this purpose, a router, called multicast router, is required to be in charge of group management in its local network. The multicast router needs to know the presence of a group in its local network. A multicast packet will be transmitted in a local network if the specified group has at least one member in that local network. IP assumes that the underlying link layer distributes the packet to the members of the multicast group. Wide area multicasting is supported via multicast routing protocols. These protocols need the group presence list of each network in order to build the multicast tree. The IGMP provides this list to the multicast routing protocols.

IGMP is based on a query/report model. The multicast router periodically sends a *query* message to all hosts address. On reception of a query message, each host sends a *report* message for each group in which it participates. A report message for a group is sent to the group address so that every group member can hear it. On reception of the first report message for a group, other group members suppress their membership report for that group. The multicast router updates its group membership list after receiving each report message. If no report message is received for a group after several query messages, the router assumes that there is no group member in its local network and deletes the group from its list.

The IGMP mechanism for group membership management is well adapted to classical LANs where bandwidth is not a scarce resource and a native broadcast mechanism is available at the link layer. A wireless LAN differs from a wireline LAN in many aspects. A wireless network is physically divided among different cells managed by different APs. An MT local to an AP can not receive the data from the other AP, although the two APs are located on the same IP subnet. Therefore, the MTs located in the same cell can only hear the data coming from their AP. Hence, the M-router must send a query message per AP in order for all the MTs to hear the message. On the other hand, the report message sent by an MT can not be heard by other MTs immediately and a loop-back mechanism is required for the M-router to retransmit the message to all MTs.

In IGMP, a host wanting to join a group, sends an unsolicited report message for that group. Leaving a group does not require any explicit action. This introduces a leave latency between the time when a host, which is the last member of a group, really leaves the group and the time when the multicast router detects the situation and stops forwarding multicast traffic. IGMPv.2 [8] attempts to decrease this latency time by introducing a leave message. A host, wanting to unsubscribe itself from a group, sends a *leave* message if it is the last member of the group. Although, even in this case the router must send a query specific message for that group in order to make sure that there is no other member of that group in its local network. Since the query messages are not sent reliably, the multicast router must repeat them several times before assuming the group absence in its local network. For IGMPv.2 the leave latency can be calculated as $R.T$, where R is the Robustness factor which is the number of times a group specific query is sent by the multicast router before assuming the group absence and T is the timeout duration which is the time between group specific query messages.

The Robustness factor R, defined in IGMPv.2, can be tuned by the network administrator according to the expected packet loss on the subnet. Choosing an optimal value for R is quite difficult due to the variable nature of error rate in wireless links. Packets may experience different error rates due to the fading effects. On the other hand, link layers are normally equipped with error control mechanisms because of the high error rate of radio interface. Therefore, it is possible that the IGMP packet goes under several retransmissions at the link layer before being accepted due to errors. This may cause the IGMP to decide that there is no member of the group in its local subnet, while the link layer is trying to get the packet across the link.

[14] proposed a mechanism to decrease the leave latency of IGMP, based on prediction techniques. The multicast router maintains a history of the last queries outcome. On reception of a leave message, the router tries to predict the outcome based on the recorded history. It also sends a query message in order to make sure about the correctness of its prediction. In a wireless environment we have a high error rate. Therefore, the probability to have a corrupted history is higher than the fixed links, specially in the case of fading when normally it takes some time before the channel returns to a better state. This scheme does not suppress the

periodic transmission of query messages causing the waste of bandwidth and a high power consumption in a wireless network.

[15] proposed an explicit join/leave mechanism to control group membership for mobile hosts. An MT sends an explicit *join* message when it wants to receive data from a group. It sends a *leave* message when abandoning a group. The existing report and leave messages in IGMPv2 can be used as explicit join and leave messages accordingly. The robustness of the protocol is assured by the router sending an acknowledgement when receiving a join or leave message. If the MT does not receive an acknowledgement from the router after a certain timeout, it repeats its join or leave request. This approach eliminates the leave latency. It is well adapted to a wireless network because of its bandwidth savings and low power consumption in the MTs.

IV. Wireless Multicasting Scheme

The essential design criteria for a multicasting scheme in a wireless network is to avoid the waste of bandwidth and to use broadcast nature of radio for multicast traffic delivery. In order to fulfill these design criteria, we propose a specific group membership protocol, that we call Wireless Group Membership Protocol (WGMP), based on the explicit join/leave mechanism described in the last section. An MT sends a join or a leave message in order to subscribe or unsubscribe itself to a group. These join and leave messages are confirmed by an acknowledgement message.

As stated before, IGMP requires the multicast router to maintain a list of groups present in its local network. This group presence list is not sufficient for an optimized multicast communication in a wireless network. In order to avoid the waste of bandwidth, multicast packets must be forwarded only to the APs with active members of the specified group. This necessitates the M-router to keep more information than the list of present groups in its local network. [1] proposed the idea of keeping a host view per multicast group. A host view of a group represents a set of cells in which every member of the group resides. Thus, instead of individually following each MT which belongs to a group, the group location is tracked.

In our system, the M-router keeps a Group Location Information (GLI). Each group, that has a member in the local network, must have an entry called location list in the GLI. A location list contains a set of APs. An AP belongs to the location list of a group if at least one MT belonging to that group is located in its cell. Therefore, whenever there is traffic destined to a group, the M-router consults the location list of the group in the GLI. It then forwards the traffic only to the APs existing in the group location list. The M-router stops forwarding data to a group whenever the group location list is empty in the GLI. In this case, the M-router must also prune itself from the corresponding multicast tree. The GLI may be updated either because of terminal mobility or because of membership changes. Changes due to terminal mobility are discussed in the next section. Membership changes cause an update of the GLI in two cases: first join case and last leave case. The first join case corresponds to the situation when an MT sends a join demand for a group that has no member in its AP. In this case, the corresponding AP must be added to the group location list. The last leave case corresponds to the situation where an MT, which is the only member of a group in its AP, sends a leave message for the group. In this case, the corresponding AP must be deleted from the group location list.

In order to support wide area multicasting, the WGMP must provide the list of groups present in its local network to the multicast routing protocols. This list can be easily generated from the GLI. A group is present in the local network if its location list is not empty. In other words, a group is present in the local network if it has an entry in the GLI.

As it is depicted in figure 2, two scenarios can be considered for group membership processing: centralized and distributed. In the centralized approach, the M-router has a central control of group membership management in its local network. For this purpose, it processes all join/leave messages coming from MTs. It must detect the first join and last leave cases in order to update the GLI accordingly. The AP does not have any control over group membership management. Its only role is to forward the multicast control messages to the M-router.

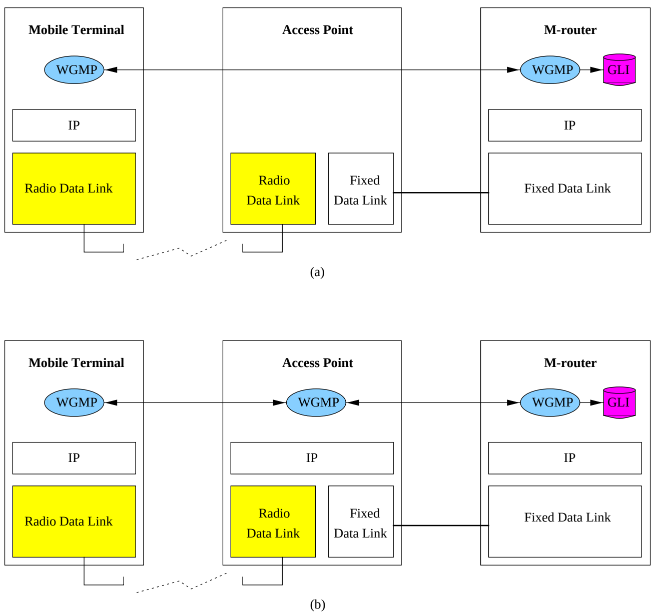

Figure 2: Group membership management.
(a) Centralized approach. (b) Distributed approach.

The distributed approach proposes to process group membership in the AP. Each AP is responsible to control the group membership state of the MTs located in its coverage area. In this case, join or leave demands coming from an MT are processed in its AP. On reception of a join message for a group, the AP must verify if the MT sending the message is the first member of the group. If this is the case, the AP subscribes itself to the group by sending a join message to the M-router which will add the AP to the group location list. In the same way, on reception of a leave message for a group, the AP must decide if the MT sending the message is the last member of the group. In this case, the AP unsubscribes itself from the group by sending a leave message to the M-router. The M-router will simply delete the AP from the group location list.

Note that on the centralized approach the M-router processes all join/leave messages sent by MTs. On reception of these messages, it decides whether or not to update the GLI. Thus, not all the join or leave messages cause an update in the GLI. On the distributed approach, it is proposed to make these decisions in the APs instead of the M-router. Therefore, the join/leave messages sent from the AP to the M-router are considered as authoritative commands causing the M-router to update the GLI immediately.

The advantage of the centralized approach is its simplicity in the APs. However, the processing load in the M-router may become quite high if there are a large number of join and leave messages in the network. The advantage of the distributed approach is that the processing load of the group membership protocol is distributed among the APs. The decisions to update a group location list are made in APs relieving the M-router from the extra processing load. The M-router just executes the update commands coming from APs. Thus, the number of multicast control messages traversing the link between the AP and the M-router are highly reduced. This scheme necessitates the APs to be IP aware. The added complexity in the APs can be justified if there is a large number of groups with high membership dynamics present in the local network. The choice between these two schemes is a tradeoff between adding complexity to the M-router or to the APs depending on the system requirements.

V. THE EFFECT OF MOBILITY ON MULTICASTING

Let us first consider the intra-domain case where an MT makes a handover to an AP under the same network domain. In this case the IP layer is unaware of terminal mobility since the MT does not change its IP address. Host mobility will cause an update in the location list of a group either if an MT, which is the last member of the group in its AP, leaves its cell or if an MT enters a cell which has no member of the group. If a group has no other member in the old AP, the M-router must delete the old AP from the group location list. The M-router must add the new AP to the location lists of those groups that have no members in its cell. Figure 3 shows an example of an intra-domain handover.

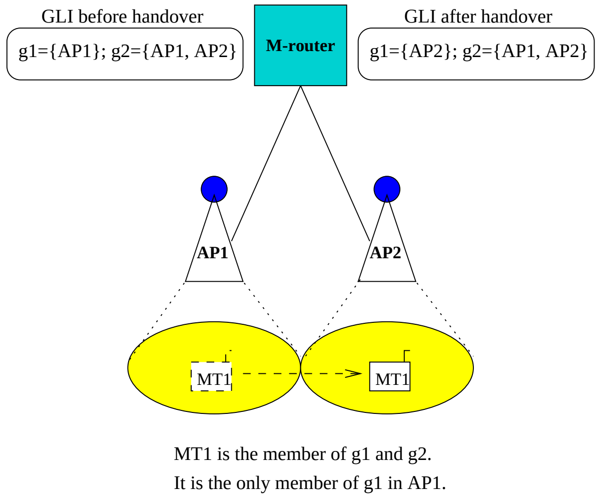

Figure 3: Intra-domain handover.

The situation is more complicated in case of inter-domain handover, where the MT moves to an AP outside its current network domain. We consider that the foreign network is also managed by a WGMP to avoid incompatibility problems. Inter-domain handover follows the IPv6 mobility functions as stated before. The location list is updated in exactly the same way as in the intra-domain handover case. Here the important issue is the mechanism for the MT to send or to receive multicast traffic in a foreign network.

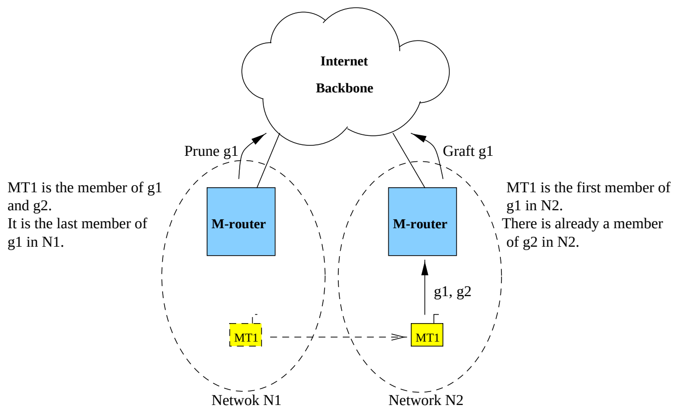

Figure 4: Inter-domain handover.

When entering a foreign network, the MT has two possibilities to receive multicast traffic. It can receive it via its HA. This requires the HA to be a multicast router. Therefore, all the join and leave messages coming from MT are processed in the HA. This approach leads to sub-optimal routing where all multicast packets must first be sent to the mobile terminal's HA and then tunneled to the foreign network. The other disadvantage is that the HA must be aware of the list of all group members in its domain in order to unicast the multicast traffic to each of them. This approach is specially not desirable for the real time applications due to the extra delay caused by the triangular routing.

The other solution is that the MT rejoins its multicast groups from the foreign network. The foreign network executes the group membership protocol and delivers the multicast traffic to the MT directly. This approach is preferable to the first one because of its optimal routing and efficient bandwidth consumption. However, the MT risks to loose packets during handover. This is due to the fact that when an MT, that belongs to a group, enters a foreign network with no member of that group, it can not receive the group traffic immediately. The local multicast router needs to graft a path to multicast trees for that group with respect to all active sources. This situation is depicted in figure 4. The packet losses can be avoided by the previous router acting as a HA and forwarding the multicast traffic to the MT.

In the same way, the MT can send a datagram to a multicast group in two ways in a foreign network. It can send it either via its HA using its home address or directly on the foreign network using its care-of-address. The first approach leads to sub-optimal routing and extra delay due to the fact that datagrams must be forwarded to the HA first. The second approach is optimal in bandwidth use and routing. The MT must use its care of address as the source IP address when sending datagrams directly from its foreign network. However, the MT changes its care of address according to its location in the Internet. Therefore, a mechanism is needed for the recipients to know that although two multicast datagrams contain different source addresses, they originated from the same mobile sender which has moved across different networks. IPv6 introduced a new header field called *destination options* header. This header field contains the options which are processed only at the destination points. We propose that the MT uses its home address in the destination options header field of an IPv6 datagram when sending multicast traffic in a foreign network. The receivers can, then, identify the sender by its home address.

VI. MULTICASTING IN WAND IP ACCESS SYSTEM

Figure 5 depicts the functional architecture of the WAND reference IP system. The system is based on the IPv6 protocol due to its facilities for mobility management and its support of QoS. The M-router has a full functionality of a standard IP router plus some enhancement for radio level mobility management. It also contains the home agent functionality in order to support inter-domain handover. The M-router controls the APs in its domain. The APs are not IP aware. They are responsible for radio resource management. The MT is a standard IP host with mobility management protocols. The radio sub-system contains basic MAC layer functionality and control functions, such as link layer mobility management and signaling. The mobile terminal includes ATM layer between link layer and IP layer because the applied radio sub-system (WAND radio) is designed for transmitting ATM cells. In the data plane, the ATM fixed size cells has been retained due to its efficient multiplexing and forwarding speed. It has been shown that the small fixed size nature of ATM cells is well suited to high speed radio interfaces [9]. The AAL5 layer segments the IP packets into ATM cells which are then forwarded by the AP transparently from the MT to the M-router and vice versa. However, the ATM connection-oriented control protocols have been discarded because of their complexity and high overhead.

The APs do not make any IP level processing. Hence, a centralized approach has been taken for group membership management by adding the WGMP instances in the MT and in the M-router. Here the main idea is to keep the AP as simple as possible.

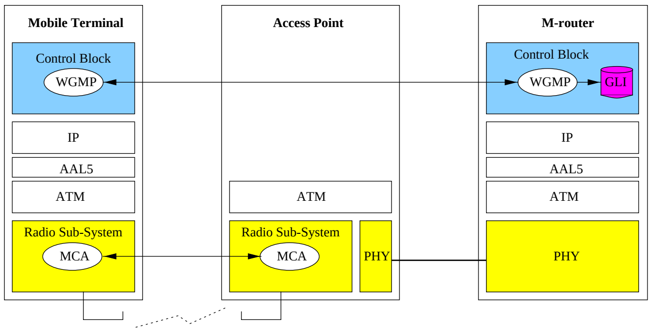

Figure 5: Architecture of WAND reference IP system.

The radio sub-system of WAND provides a link layer addressing scheme. Each MT is identified by a link layer address in the AP. This address is given by the AP to the MT and is unique in the range of a single AP. The link layer addressing scheme can be similarly used to identify a multicast group in the AP. The radio sub-system also provides some facilities for broadcast channels. These facilities together with link layer addressing of multicast groups can be used for efficient and bandwidth saving transmission of multicast traffic.

The mechanism is as follows. The M-router orders an AP to allocate a link layer address to a group whenever there is a join demand for a group that does not have any member in that AP. The AP uses this address to identify the group as long as the group has at least one member in its cell. This address is communicated by the AP to its local group members. The group members, in turn, memorize this address for further use. The AP delivers traffic coming for a group using the link layer address of the group. Therefore, only the MTs which are aware of this address will receive the multicast traffic. Other MTs simply discard the traffic since it has not been destined to them. In consequence, multicast communication requires some modifications in the radio link layer. The MultiCast Agents (MCA) added to the radio sub-system of the MT and the AP are responsible for the multicast functionality in the link layer, as it is shown in the figure 5.

In case of handover, multicast communications are essentially handled in the same way as it is described in the last section. The M-router updates the group location list if necessary. In addition, if a group has no other member in the old AP, its link layer address as well as all its active connections must be released. On the other hand, the new AP must allocate new link layer addresses to those groups that have no members in its cell. In the inter-domain handover case, the MT must rejoin its multicast groups in its foreign network. The foreign network executes WGMP and delivers multicast traffic to the MT in exactly the same way as to its local MTs. The MT sends multicast traffic directly in its foreign network using its care-of-address as its source IP address and its home address in the destination options header field.

VII. CONCLUSION

We presented a general framework for multicast communication in wireless networks. In our design, we tried to minimize the bandwidth use and the power consumption of mobile terminals which are the two main constraints in a wireless network. We presented a specific group membership protocol called WGMP. This protocol is based on join/leave model. We proposed that the M-router maintains a location list per group. The location list of a group contains the set of APs having at least one member of the group in their cells. This scheme avoids forwarding the traffic destined to a specified group to the APs with no member of that group. We also studied the interoperation of multicast communication and mobility. Finally, the wireless IP access system of WAND was taken as a case study. The developed multicasting scheme has been applied to WAND IP architecture. We took advantage of the link layer addressing scheme of WAND radio sub-system as well as its facilities for broadcast channels to deliver multicast traffic in an efficient way with a single transmission.

ACKNOWLEDGEMENTS

This work has been performed in the framework of the project ACTS AC085 The Magic WAND, which is partly funded by the European Community and the Swiss BBW (Bundesamt für Bildung und Wissenschaft). The authors would like to acknowledge the contributions of their colleagues from Nokia Mobile Phones, Lucent Technologies, Tampere University of Technology, Technical Research Centre of Finland, Ascom Tech AG, University of Lancaster, Robert Bosch GmbH, University of ULM, Compagnie IBM France, IBM Zürich Research Laboratory, Eurecom Institute, ETH Zürich, Intracom Hellenic Telecommunications and University of Athens.

REFERENCES

[1] A. Acharya, and B. R. Badrinath, "A Framework for Delivering Multicast Messages in Networks with Mobile Hosts" , Rutgers DCS TR-310, 1994.

[2] J. Ala-Laurila, L. Stacey, N. Nikaein, and J. Seppälä, "Designing a Wireless Broadband IP System with QoS Guarantees", ACTS Mobile Summit, Greece, June 1998.

[3] The ATM Forum Technical Committee, "LAN Emulation Over ATM", January 1995.

[4] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF Internet Draft, Work in Progress, November 1997.

[5] S. Deering, and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", IETF RFC 1883, December 1995.

[6] S. Deering, "Host Extensions for IP Multicasting", RFC 1112, August 1989.

[7] C. Diot, W. Dabbous and J. Crowcroft, "Multipoint communications: a survey of protocols, functions and mechanism", IEEE JSAC, vol. 15, no. 3, April 1997.

[8] W. Fenner, "Internet Group Management Protocol, Version 2", RFC 2236, November 1997.

[9] T. Freeburg, "Wireless ATM: Introduction to Mobility and Related Issues", Presentation at Nomadic '97, August 1997.

[10] D. Johnson, and C. Perkins, "Mobility Support in IPv6", IETF Internet Draft, Work in Progress, March 1998.

[11] J. Mikkonen, and J. Kruys, "The Magic WAND: a Wireless ATM Access System", ACTS Mobile Summit, Spain, November 1996.

[12] C. Perkins, "IP Mobility Support", IETF Standard Track RFC 2002, October 1996.

[13] C. Perkins, and D. Johnson, "Mobility Support in IPv6", MOBICOM'96, November 1996.

[14] L. Rizzo, "Fast Group Management in IGMP", HIPPARCH'98 workshop, June 1998.

[15] G. Xylomenos, and G. Polyzos, "IP Multicast for Mobile Hosts", IEEE Communications Magazine, January 1997.