

Supporting Multicast in Ad-Hoc networks in a Hotspot Context

Andreas Kassler¹, Susana Sargento², Adel Ben Mnaouer³, Chen Lei³, Pedro Neves², Rui L. Aguiar², Pedro M. Ruiz⁴

¹ Karlstad University, Sweden

² Instituto de Telecomunicações, Universidade de Aveiro, Portugal

³ Nanyang Technological University, Singapore

⁴ University of Murcia, Spain

Abstract

This paper discusses the usage of Ad-Hoc technologies as “hotspot extension” mechanisms. We propose a hybrid network where 802.16 links are used for providing high-bandwidth access, and local distribution is performed by Ad-Hoc network nodes (based on 802.11 technologies), thus covering arbitrary areas around the 802.16 stations, which might be connected to the Internet. We evaluate the performance of the system and its efficiency in providing QoS in multicast connections. For providing multicasting services, we propose two extensions of the ODMRP and MAODV routing algorithms by augmenting them with a zone routing behavior, thus producing two new hybrid multicast routing algorithms, named ZODMRP and ZMAODV. The simulation results show that ZODMRP provides the highest packet delivery ratio and lowest delay without introducing large overhead, being then able to provide predictable QoS for packet delivery in multicast sessions.

1 Introduction

Ad-Hoc networks have gone through large developments over the last years. Researchers have investigated aspects of routing, multicasting, QoS and security in these networks. Currently, Ad-Hoc is reaching a stage where they can support the mixing of different services in order to provide an infrastructure useful for the common user.

One such service is the basic network connection. Future users will be permanently connected, not only to their local environment, but also to the overall Internet. The “hotspot” concept is a clear indication of this trend, with more and more access points available for public usage. With the increased desire to be always connected, this concept will be certainly enlarged to an “extended hotspot” concept. The idea is to increase the range of hotspots through the automatic creation of Ad-Hoc networks based on connections to nodes increasingly nearer the hotspot range.

This scenario is particularly useful for users and operators: telecom operators associated with wireless subscriber access still provide general network access, and the users cooperate to overcome the limitations of the operators limited coverage, and create a virtual hotspot. These “hotspot” scenarios, often discussed

with satellite technologies, rely on a set of key access points with high bandwidth, which act as repeaters for users nearby. We propose such a hybrid network where 802.16 links [1] [2] are used for providing high-bandwidth access, and local distribution is performed by multi-hop Ad-Hoc networks using IEEE 802.11. This allows for the covering of arbitrary areas around the 802.16 stations. Recent announcements of intrinsic laptop support for both 802.11 and 802.16 technologies [2], and the proposals of incentive-based charging schemes for Ad-Hoc networks [3], make this scenario quite feasible in the near future.

The paper discusses this scenario and analyzes multicast services on this environment. We discuss the usage of MAODV (Multicast Ad-Hoc On-demand Distance Vector protocol) and ODMRP (On-Demand Multicast Routing Protocol) and variants to provide multicast support. The smooth integration of these different protocols and proposed evolutions will be presented. Furthermore, the adequate mapping of multicast requirements in the distribution 802.16 technology will also be discussed.

This paper is organized as follows. In section 2 the proposed overall network architecture is presented, as well as its main sub-networks (the wired and infrastructure access network, the 802.16 access network and the mobile 802.11 Ad-Hoc networks). Section 3 addresses the 802.16 distribution network and the multicast mapping into 802.16 technologies. Multicast proposals in Ad-Hoc networks and their integration with infrastructure networks are described in section 4. Simulation results are presented in Section 5. Finally, Section 6 reports the main conclusions.

2 Network Architecture

Mobile telecommunication networks are facing novel paradigms. With an increasing desire to access information on the Internet and to access any information anywhere, current trends push to the integration/merger of the Internet and mobile networks. A particularly hot area of Internet mobility is Ad-Hoc networking. These networks are temporarily formed, without any infrastructure, with nodes dynamically

joining and leaving the network. Although Ad-Hoc networks were primarily seen as independent networks, nowadays they can also be seen as extensions of access networks, e.g., extended hotspot scenarios, where nodes can access infrastructure networks and the Internet, through other mobile nodes.

Regardless of the increased number of hotspots around the globe, there will always be some areas that will not be covered by the hotspots. Larger areas solutions are appearing for those situations. The IEEE 802.16 is such a broadband wireless technology that provides broadband wireless access in metropolitan area networks (MAN) [1] [2]: it will be able to deliver wireless and high-speed connections worldwide, replacing the existing wired broadband connections. Furthermore, 802.16 will be able to support non-fixed nodes in a near future, bringing mobility into this MAN scenario.

Our proposal is to use 802.16 as an extension of access networks, providing high bandwidth access between the terminals and wired access network, and then extend this access by the creation of Ad-Hoc networks over 802.11. This situation can appear either with operator-owned hotspots or with dynamic situations, where a 802.16/11-enabled user acts as the gateway between the telecommunications operator and the other users. Figure 1 depicts the proposed network architecture, able to provide high bandwidth access through the 802.16 distribution networks, and with local 802.11 Ad-Hoc networks in each 802.16 station.

In the top of the network it is depicted the infrastructure and wired access network. The access router can be directly connected to the 802.16 base station (BS). As a broadband wireless access technology, 802.16 is intended to be used as a bridging solution between the access network and the backhaul wireless access technologies. Namely, in this scenario, 802.16 provides broadband wireless access to 802.11 wireless networks working in Ad-Hoc mode. As shown in the figure, each one of these 802.11 Ad-Hoc networks is connected to the 802.16 technology through the (eventually fixed) subscriber station (SS) units.

Each Ad-Hoc node is connected to the access point through a multi-hop path composed by mobile nodes in the Ad-Hoc network. We consider that the target mobile nodes in this network are laptops and personal digital assistants (PDA). In 802.16 each subscriber station includes (currently) a rooftop-mounted antenna unit connected to an indoor network interface unit. Using a single base station, the Wireless Internet Service Provider (WISP) is able to cover broad geographic areas, supporting 250 subscriber stations in

each one of the base station sectors. In the future, this 802.16 support can be provided directly by high-end laptops.

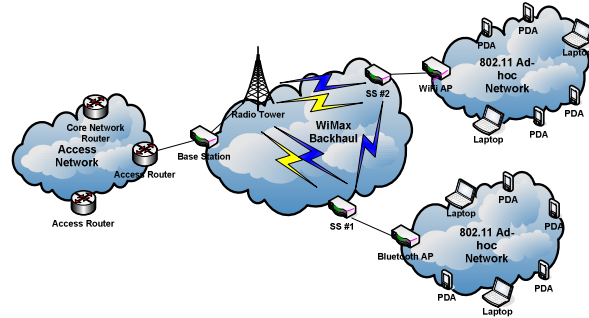


Figure 1: Network Architecture

Both point-to-multipoint and mesh topologies are supported by 802.16 and illustrated in Figure 1. The point-to-multipoint topology is illustrated using yellow communication links and the mesh topology is shown using blue communication links. The operators are able to choose one of these two different topologies in order to fulfill its traffic requirements. In the point-to-multipoint topology, the downlink traffic is generally broadcasted and all subscriber stations listen to it. However, it is possible to assign a specific burst of information to a specific subscriber station (unicast burst) or for a specific group of subscriber stations (multicast burst). In this topology, subscriber stations are not able to communicate directly between them. If a subscriber station wants to forward traffic to a peer subscriber station, the traffic must be sent through the base station. In the uplink direction, the subscriber stations must forward the traffic to the base station in an on-demand basis, depending on the used uplink scheduling service. On the other hand, the mesh topology allows the subscriber stations to communicate directly between them, avoiding forwarding all of its traffic to the base station. As we can see in Figure 1, in mesh networks, two important entities are represented: the mesh BS and the mesh SS. The mesh BS is the BS that has a direct connection to the backhaul services outside the mesh network. The mesh SS are all the other SSs that belong to the mesh network (SSs 1, 2 and 3).

The purpose of this network is to be able to deliver and support any type of services and applications, as audio and video conferencing and streaming, to the end users, located in any hotspot network connected to the Internet through broadband wireless. Since the access network is composed by wired and fixed network, 802.16 distribution network and wireless Ad-Hoc network, these networks need to be closely integrated to provide the services delivery.

3 Packet distribution in 802.16

In 802.16 networks, packets traversing the MAC interface are associated to a service flow as identified by a Connection Identifier (CID) that has some pre-defined treatment. This association is provided by a classifier both in the SSs and in the BS. Moreover, each service flow will have assigned resources between SS and BS that will last for the duration of the connection. These mechanisms, that will be further detailed, will allow the basic support of multicast in 802.16.

In the 802.16 context, a connection is a unidirectional mapping between the BS and the SS with the purpose of transporting service flows. Each connection is identified by a CID. A service flow is defined as a MAC transport service that provides unidirectional transport of packets either in uplink and downlink directions. Each service flow is identified by a Service Flow Identifier (SFID) and is defined by a particular set of QoS parameters (latency, jitter, and bandwidth). Several types of connections may be established between the SS and BS: three management connections, broadcast and multicast connections, and several transport connections. During the network entry and initialization, each SS is assigned with three management connections in each direction: (1) basic connection used for the transfer of short, time-critical MAC management messages; (2) primary management connection used to transfer longer, more delay-tolerant messages; and (3) secondary management connection used for the transfer of delay-tolerant standards-based management messages. Broadcast management or data connections are also used to transmit MAC management messages or data messages to all the SSs. A multicast polling connection is also used by the SS to join multicast polling groups and to request bandwidth via polling. In addition to these connections, transport connections are allocated to the SSs for the contracted services.

Regarding mesh networks, each node that belongs to this particular type of network shall receive a node identifier (Node ID), transmitted upon a request to the mesh BS. Each node shall assign a Link Identifier, transmitted as part of the CID, to each link it establishes with its neighbors. In the mesh topology several types of scheduling are defined to coordinate the transmissions and avoid collisions between the mesh SSs and between the mesh SSs and mesh BSs.

4 IEEE 802.16 Multicast

While in 802.16 networks broadcast management and data connections are supported, there is no explicit

multicast data transport connection defined. Instead, a range of connections is defined for multicast polling. These connections are used for the SSs to join multicast polling groups. Concerning multicast data transport connections, although there is no dedicated connection, it is possible to have a multicast connection for data.

The process for setting up a multicast connection is as follows. The BS should have information on the mobile nodes joining a multicast group. This can be provided by e.g. the access router (see Section 5.2). Then it is responsible to setup a multicast group inside the 802.16 network. To accomplish this task, the BS starts to create and associate a unicast transport connection with a specific SS. Then, this same connection is associated with all the SSs that belong to the multicast group. With this process, when multicast traffic is sent on this connection, all the SSs that belong to the multicast group are able to listen to this traffic. Inside Ad-Hoc networks, Ad-Hoc multicast routing protocols, as MAODV or ODMRP, are used to manage the multicast groups. The multicast connection is illustrated in Figure 2. Consider a multicast group with four elements (1 laptop in SS#1, 1 PDA in SS#1 and 2 PDAs in SS#3). In this case, a unicast transport connection is established between the BS and SS#1 (0xFEFC). After this connection is established, the BS creates a similar unicast transport connection with SS#3 using the same connection identifier (CID = 0xFEFC). This way, both SS#1 and SS#3 start listening to data sent on this connection. Thus, we have a multicast connection established between the BS, SS#1 and SS#3.



Figure 2: Multicast in 802.16

It is important to mention that an 802.16 multicast connection is only required if the multicast nodes belong to different SSs. This is the situation illustrated in the example. However, if the multicast group elements all belong to one SS, no 802.16 multicast

connections would be required in this case. A simple unicast connection would be enough to send data to the multicast group only formed inside the Ad-Hoc network.

5 Ad-Hoc Network Multicast Integration

In multicast communications a source is sending only one packet with a group address as a destination. The network will be in charge of replicating that packet only when necessary to make it reach all the destinations, i.e. all the nodes that have joined the group associated with that specific group address. This leads to minimal bandwidth consumption and high scalability. Support for multicast is thus essential in hybrid Ad-Hoc networks in which the bandwidth and the power in the mobile nodes are limited. The classical IP multicast protocols used in the Internet consists of the Internet Group Management Protocol (IGMP) [4] for group membership (or its IPv6 variant MLD) in combination with an IP based multicast routing protocol like Protocol Independent Multicast - Sparse Mode (PIM-SM) [5]. Because of Ad-Hoc network specific problems like frequent topology changes, unreliable links, battery constraints and limited capacity of mobile nodes, standard internet multicast routing protocols, introducing high overhead in maintaining efficient multicast delivery structures, do not perform well regarding scalability and performance in Ad-Hoc networks, especially when trees need to be re-organized frequently due to mobility. The benefits of multicast include the lower bandwidth consumption and increased scalability. Therefore, the support of multicast is essential in Ad-Hoc networks, since the bandwidth and the power of the nodes is limited.

5.1 Multicasting in Ad-Hoc Environments

Specific multicast routing protocols have been designed for Ad-Hoc networks, which can be classified according to the placement of the multicast delivery structure. In addition to pure flooding, which leads to a very high overhead in Ad-Hoc networks, we can distinguish between tree, mesh and location based multicast routing mechanisms. AMRoute [6], AMRIS [7], or MAODV [8] delivery structure is tree based. While AMRoute creates a bi-directional shared core-based tree using unicast tunnels, it uses virtual mesh links for tree creation and needs a unicast routing protocol. This results in temporary loops and sub-optimal routes with mobility. The approach of AMRIS is to use a shared tree and an ID number per node. It does not depend on a unicast routing protocol. New-session messages are

broadcasted and it uses beacons to detect disconnection and re-joins to potential parents. However, it does not scale well as it uses expanding ring search mechanism for branch re-construction due to node failure.

ODMRP [9] and CAMP [10] are mesh based. While CAMP uses a shared mesh, and all nodes keep membership, routing and packet information, it needs a special unicast routing protocol. New members use expanding ring search to find other member neighbors. In contrast, ODMRP floods packets within a mesh, but follows an on-demand policy for establishment and update of the mesh. ODMRP is based on request and reply phases, where sources broadcast announcements, and it does not require unicast routing. The mesh is created when join requests from multiple receivers are sent to multiple-sources. This results in tree-like structures for sparse groups or single-sender which leads to problems with robustness. A local route recovery scheme can be used to address this problem. The motivation for mesh based approaches is due to the problems with tree-based approaches in the presence of mobile nodes because tree-structures are fragile and need to be frequently readjusted when connectivity changes. Using delivery meshes that span all multicast group members, multiple links do exist which provides redundancy to route breaks caused by mobility of nodes. This minimizes packet loss and avoids frequent tree re-organization but leads to higher overhead due to redundant transmissions wasting energy in battery operated mobile nodes.

Multicast Core Extraction Distributed Ad-Hoc Routing (MCEDAR) [11] is a multicast extension to CEDAR. MCEDAR incorporates the efficiency of tree-based forwarding protocols and robustness of mesh-based protocols by combining them. Therefore, it decouples the control infrastructure from the actual data forwarding. Due to the usage of a mesh delivery structure, it tolerates a few link breakages due to mobility without the need to reconfigure the whole mesh. The forwarding mechanism on the mesh creates an implicit route-based forwarding tree which makes the protocol efficient.

Finally, in location-based multicasting (e.g. [12]), location information (available by e.g. Global Positioning System - GPS) is used to define group membership and distribute multicast traffic. These protocols can use simple flooding techniques within the forwarding region, which might be more efficient in some situations than multicast routing.

Traditional (multicast) routing protocols for Ad-Hoc networks have not been designed to interoperate with fixed networks due to several reasons: The addressing architecture is different in Ad-Hoc networks, in which

host-based routes are commonly used and addressing structure is flat compared to a hierarchical structure in the internet. In the Internet, two nodes sharing the same network part of their IP addresses are assumed to be in the same link, which is not necessarily the case in multihop networks. Classical internet multicast protocols offer superior performance in fixed networks than pure Ad-Hoc solutions, which are designed for frequent topology change. Due to these reasons, it is hard to design a multicast protocol that works efficiently in the Ad-Hoc part while still being able to interoperate with the fixed network. Therefore, it is desirable to design inter-working between Ad-Hoc and internet multicast protocols to achieve the best performance.

Very little efforts, if any, have been started to provide multicasting in such hybrid Ad-Hoc networks. The SAFARI project [13] developed a solution which supports multicasting to mobile nodes through the usage of MLD proxy and integrates it with Mobile IPv6. A MLD proxy, when installed on a Mobile IPv6 Home Agent (HA), can receive MLD reports sent by one of its mobile nodes. A tunnel is setup between the HA and the MN. The MN can therefore send MLD reports to the HA via the tunnel. The MLD proxy traps such reports and joins (from its own LAN) the multicast group(s) on behalf of the mobile nodes it serves. The multicast data is then forwarded to the current location of the MN. If the MN is within an Ad-Hoc network, broadcasting is used for the multicast delivery in the Ad-Hoc portion, which is very inefficient. In [14], a multicast gateway (MGW) has been proposed to support multicast routing for MANETs connected to the fixed internet. The MGW is in charge of translating between the multicast routing protocols used in the fixed portion and those protocols used in the Ad-Hoc fringe. This is clearly a big drawback as the gateway must be aware of the multicast protocol deployed in the Ad-Hoc network. Also, it is not straightforward to extend the work in [14] so that several MGWs can be supported, an important feature to provide resilience and survivability. It also does not allow a standard multicast client located in the Ad-Hoc fringe to participate in the communication. Also, it remains unclear how Ad-Hoc multicast receivers are informed about groups in the fixed portion of the network.

5.2 Integration of Ad-Hoc Networks with the public Internet

Standard Ad-Hoc multicast protocols (like ODMRP or MAODV) have been proposed particularly for Ad-Hoc networks, which incorporate specific mechanisms to

efficiently operate in stand-alone Ad-Hoc networks. However, they can neither interoperate with a fixed IP network nor support standard-IP multicast sources or receivers. In our scenario, where Ad-Hoc networks are connected through 802.16 with the internet, several extensions are required. These extensions must be designed in such a way that they are compatible with the standard IP Multicast mode, and they must allow standard IP nodes to take part in multicast communications without requiring any change. Therefore, an Ad-Hoc multicast routing protocol should support IGMP as a means to interoperate both with access gateways and standard IP nodes. In addition, the 802.16 BS must be enabled to setup a multicast group inside the 802.16 network, which requires information about what members of which multicast group are attached to what 802.16 SS.

We propose that all nodes in the Ad-Hoc fringe situated just one hop away from the gateway (denoted as Multicast Internet Gateways - MIG - in the Multicast MANET Routing Protocol – MMARP - [15] terminology) notify the access routers about the group memberships within the Ad-Hoc fringe. Any node within the Ad-Hoc fringe may become a MIG at any time if that node receives IGMP reports from multicast routers in the Access Network, because IGMP messages are sent with TTL=1. This requires in our architecture that the 802.16 network does not change the TTL of IGMP messages. This mechanism allows the multicast Ad-Hoc routing protocol to work with any IP multicast routing protocol in the access network and, therefore, it shields the multicast Ad-Hoc routing protocol operation from the protocols performing the intra-domain or inter-domain multicast routing. Therefore, MIGs must periodically advertise themselves to all other Ad-Hoc nodes as default multicast gateway to the fixed network. Ad-Hoc nodes can determine if they have to advertise themselves as MIG by receiving IGMP queries from the access router attached to the 802.16 BS. Such advertisement messages broadcasted from MIGs inform intermediate Ad-Hoc nodes about the path towards multicast sources in the access network, and thus the global internet. When such an advertisement reaches a receiver or neighbor of a receiver of a multicast group within the Ad-Hoc part, this node has to initiate a joining process using the multicast Ad-Hoc routing protocol towards the MIG. Once the MIG receives the request from an Ad-Hoc node to join, it sends an IGMP Report towards the access router thus updating group membership information. This ensures that IP multicast data from sources in the fixed network reach the destinations within the Ad-Hoc network. Also, the access router

then notifies the 802.16 BS, which then sets up the multicast group within the 802.16 network to forward traffic to the correct 802.16 SS and thus to the proper Ad-Hoc island.

The layer 3 multicast protocol is transparent in the 802.16 network. The BS just needs to be informed of the multicast group (through the AR), and all the multicast processing inside 802.16 network is the management of the multicast connections between the BS and SS.

If an Ad-Hoc node is becoming an active multicast source, it triggers the creation of a multicast distribution structure (tree or mesh) depending on the routing protocol in use. However, to ease network integration, the multicast Ad-Hoc specific messages should be created by the neighboring Ad-Hoc nodes which receive the data packets from the source. This might lead to the creation of unnecessary paths [15] and mechanisms need to be deployed to prevent such unnecessary message creations. If the MIGs become aware of new multicast sources in the Ad-Hoc island, they notify the access routers about this information by sending IGMP reports towards the Access Router, so again the 802.16 infrastructure should not change the TTL of IGMP messages.

5.3 Design of new Multicast Routing Protocols

When designing new routing protocols for Ad-Hoc networks, it is important to note that ZRP does not provide a single protocol, but rather outlines a *routing framework* suitable for inclusion and extension of other existing protocols. In addition, the multicast variant MZR uses a quite simple path finding process, and a source-based multicast data delivery tree. Therefore, combining the Zone Routing with reactive protocol features to form new hybrid protocols is expected to achieve good performance. Also, it has already been shown in [8] and [9] that MAODV and ODMRP present good performance. Therefore, our objective is to extend MAODV and ODMRP with a proactive behavior. The idea is that it is important to reduce the overhead especially when there are hotspots which are likely to be congested.

The new hybrid protocol contains reactive and proactive (based on zone routing) behaviors. In the proactive mode, each node in the Ad-Hoc part of the network constructs and maintains a zone around it with a pre-configured zone radius. Each node thus maintains a zone routing table to record the multicast information of the nodes in its zone by periodically broadcasting an update packet. The time-to-live (TTL) value of the packet is set to the pre-configured zone radius. Each update packet includes multicast information of the

source node (the node which is sending the update packet). The purpose of the update packet is to distribute information about the source node sending the update packet to members within its zone. In this way, any node receiving such an update packet knows immediately to which multicast groups a specific source node belongs. If such neighbors receive join requests for a specific multicast group, they can immediately determine to which source node to forward such a request. For MAODV, the update packet includes multicast group addresses that the source node belongs to, multicast group leader address, and the multicast group sequence number. For ODMRP, it includes multicast group addresses that the source node belongs to. When an Ad-Hoc node within the zone receives the update packet, it records all information in that packet, including source node address, multicast group information, hop count to the source node, and next hop address to the source node. Therefore, the zone routing table is kept up-to-date by the periodic broadcast. Each table entry has a timeout value and an entry is removed if its timer expires before a new update packet arrives.

The zone information each node recorded is most useful when a node must find a path. Therefore, we modify the way MAODV and ODMRP send out a join request. We will describe the details separately below, and the other parts such as join reply, group hello for MAODV will remain as in the original protocol. The resulting two protocol variants are described as ZMAODV and ZODMRP, respectively. We extend the architecture of Ad-Hoc nodes by introducing a zone routing table that is used to record the information of the nodes within the zone. Each entry contains information of one node within the zone, including the next hop node, number of hops, node's address, and the multicast information of this node, such as the multicast group it belongs to.

Sending RREQ in ZMAODV: When a node needs to send a RREQ, it first looks up the zone routing table to see whether there are nodes in the zone that belong to the multicast group the node intends to join. If there are already other nodes that belong to the multicast group in its zone, it compares other information, for example, multicast group sequence number and multicast group leader address, to ensure that the information recorded in the zone routing table is fresh. After that, if there are still some nodes in the zone, the source node unicasts a RREQ to the nearest node and waits for the reply. If it finds no nodes in its zone, the source node broadcasts a RREQ setting its TTL to the zone radius. Only the border nodes having hop count to the source node equal to the zone radius will handle the RREQ. All

other nodes in the zone propagate the RREQ to the border nodes. When a border node receives the RREQ, it looks up its zone routing table and continues the path finding procedure until some nodes belonging to multicast group receive the RREQ. That node will then generate a RREP and send the RREP to the source node following the reverse path.

Sending Join Query in ZODMRP: The procedure sending Join Query in ZODMRP is similar to the procedure of sending RREQ in ZMAODV. The difference is when a node finds other nodes in its zone belonging to the multicast group. In this situation it does not only unicast the Join Query to the node with the shortest path, but to all nodes belonging to the multicast group. This helps to build up the forwarding group as a mesh.

6 Evaluation: ZMAODV and ZODMRP

In this chapter, we present the results of our evaluation of multicast protocol performance in an environment, where Ad-Hoc islands are connected to the public internet. We simulated the performance of the Ad-Hoc network only as we assume the MANET to be the bottleneck and not the 802.16 backhaul network. In the future, we plan to perform a simulation at a larger scope.

6.1 Simulation Description

We used GloMoSim [16] to compare the performance of ZMAODV and ZODMRP with two Ad-Hoc multicast routing protocols, MAODV and ODMRP (for ODMRP, we did not use the mobility prediction feature of the protocol). As we are interested in a scenario where an Ad-Hoc network is connected to an infrastructure network, we set the mobility of the gateway to the infrastructure based on 802.16 to zero. These gateway nodes participate in sending and receiving several multicast groups and a gateway thus may belong to more than one multicast group at the same time. All other nodes in the Ad-Hoc network are mobile with variable speed. We distribute in total 50 Ad-Hoc nodes running 802.11 within an area of 1000x1000 m. Radio propagation range for each node is set to 250 m and channel capacity is 2 Mbps. Each simulation is executed for 500s of simulation time, which corresponds to a typical time required for video news consumption within a hotspot.

We use constant bitrate UDP sources emulating typical audio and video streams. For audio, we use 240 byte packets, sent out every 30 ms at a total bitrate of 64 kbps. For video, we use 1500 byte packets, sent out every 80 ms at a total bitrate of 150 kbps. In the

scenarios, we select one node (mobility=0m/s) to be the access point towards the 802.16 access network. This node receives traffic from three (two audio and one video) other multicast sources and forwards it to the 802.16 access network. In addition, this node also multicasts two audio and one video stream that it receives from the 802.16 network towards the Ad-Hoc nodes. Clearly, the 802.16 links are not the bottleneck and traffic is concentrated around the 802.11 access point connecting the 802.16 access network to the Ad-Hoc island.

We use the following performance metrics to compare the performance of the multicast protocols. *Packet delivery ratio*, which determines the effectiveness of the protocol (for interactive audio, packet delivery ratio must approach one for high quality experience), *Average packet delay* and *Delay Jitter* (for interactivity, delay and jitter must be minimized). Note that Average Packet Delay and Delay Jitter are averaged among all receivers of the multicast group. In addition, we distinguish between the delay experienced at the Access Point (due to higher load and traffic concentration) and all other nodes. *Number of data packets transmitted per number of data packets delivered* is the ratio of every individual transmission of data by each node over the entire network versus number of data packets delivered to the destination (the higher this ratio, the higher the overhead in terms of packet transmissions). *Number of control packets transmitted per number of data packet delivered* denotes how much control overhead is transmitted for sending the data packets.

Each node moves constantly with a randomly generated speed and moving directions are randomly selected. Nodes reaching the simulation boundary bounce back and continue to move. Although there are other mobility models available (like e.g. group mobility model), the random mobility model was selected as it stresses the routing protocols. Two different scenario setups are used. In the first setup we are interested in the protocol performance depending on the multicast group size. Here, we fixed the mobility of the nodes at 5 m/s and vary the group size between 5 and 25 members in steps of 5. In the second scenario, we fixed the multicast group size to 10 and vary the mobility of the nodes from 0 to 30 m/s in steps of 5 m/s.

6.2 Simulation Results and analysis

Figure 3 shows packet delivery ratio as a function of terminal speed. ODMRP shows good performance compared to MAODV even under high mobility. This is due to the mesh topology: the chances of packet delivery are high even if primary route is no longer

available. ZODMRP outperforms ODMRP and ZMAODV performs better than MAODV, as the proactive zone feature helps to recover broken links. This is mostly visible at high mobility for ZMAODV. More packets are dropped in the direction towards the 802.16 network (denoted as at AP) as traffic is concentrated around the AP which leads to high collision ratio. Here, also the Z-variant outperforms the standard protocols and performance improvement is best for the ZMAODV when compared to MAODV at high mobility. For providing predictable QoS for packet delivery for, e.g. audio packets, we conclude that ZODMRP is the method of choice.

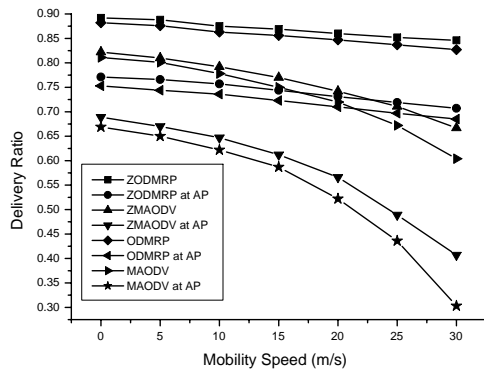


Figure 3: Packet Delivery Ratio as a function of mobility speed.

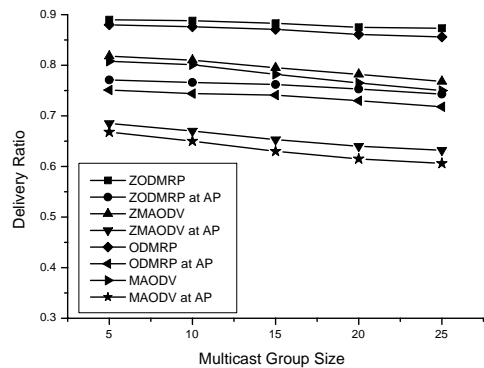


Figure 4: Packet Delivery Ratio as a function of group size.

In Figure 4 we analyze the packet delivery ratio as a function of multicast group size. Again, the behavior is similar with increasing members in a multicast group. The higher the group size, the more traffic is generated altogether and the higher the packet-dropping probability due to collisions. Therefore, ZODMRP and ODMRP outperform ZMAODV and MAODV. Again, there is a noticeable difference between the packet loss

rate as experienced by standard receivers compared to the access point (traffic direction towards the infrastructure networks), as the probability of packet collisions is higher around the AP.

Figure 5 shows the average packet delay as a function of terminal speed. This is important in order to evaluate the suitability with respect to QoS provisioning. Again, ZODMRP outperforms ODMRP, which is better than ZMAODV and AODV. Here, the performance degradation at high mobility is severe for MAODV (150 ms at 0 m/s compared to 420 ms at 30 m/s) and ZMAODV. However, the delay for ZODMRP is nearly constant and below 100 ms even at high mobility, due to the intrinsic back-up routes provided by the mesh. Again, performance is significantly lower in direction towards the access point for all protocol variants.

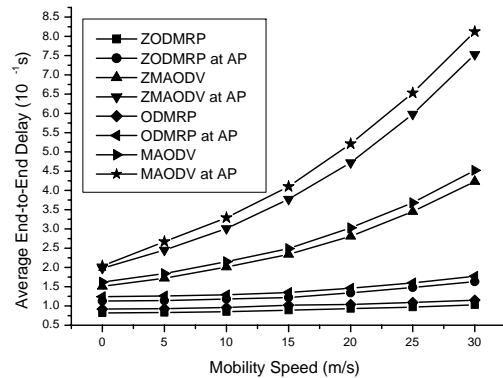


Figure 5: Average Delay as a function of mobility speed.

Figure 6 shows packet jitter as a function of terminal speed. While ZODMRP is again the protocol of choice showing similar behavior for jitter compared to delay, it is important to note that with such a high jitter as 650 ms for MAODV and its Z-variant (towards infrastructure network), it is not possible to provide QoS for interactive audio and video conferencing. In contrast, the jitter for ZODMRP is almost constant at around 50 ms and lower than jitter experienced for ODMRP (which is still below 75 ms), in direction from the access point to the nodes. In the opposite direction, towards the infrastructure network, jitter is almost independent from mobility effects at around 100 ms for both variants of ODMRP.

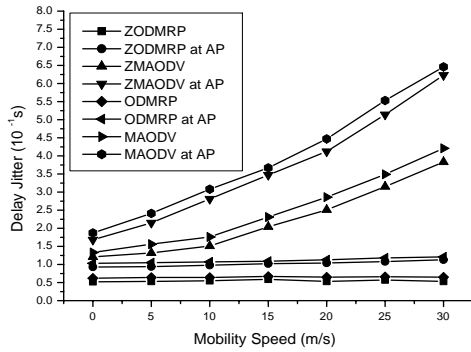


Figure 6: Average Packet Jitter as a function of mobility speed

Figure 7 shows the number of data packets transmitted per number of data packets delivered to the destination, as a function of terminal speed. Both ZODMRP and ODMRP have highest number of transmissions due to the mesh distribution structure exploiting multiple redundant routes. The MAODV loses the ground for mobility speeds higher than 15 m/s to the ZMAODV counterpart. In this figure and all subsequent ones, we do not distinguish if a packet is sent from the access point or towards it. Instead, we count the total amount of data/control packets transmitted for each protocol variant irrespective of the direction (uplink/downlink).

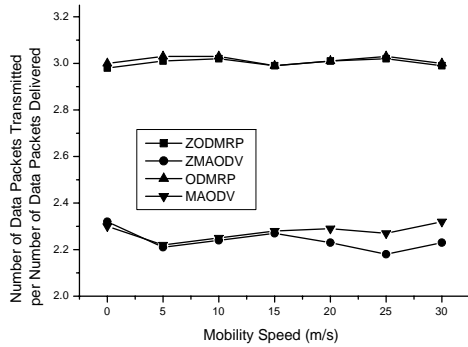


Figure 7: Number of data packets transmitted per data packet delivered as a function of mobility speed

Figure 8 plots the number of control packets transmitted per number of data packet delivered as a function of mobility speed. For high mobility speeds (above 10 m/s), the ODMRP and its Z-variant generate lower overhead than the MAODV group whose control packet generation increase sharply with higher speed. This is due to the need for larger number of control packets to cope with link breaks and repairs. Again the ZMAODV outperforms pure MAODV for fast mobility. The ODMRP/ZODMRP are more robust

against link breaks due to high mobility speed which is because of the mesh topology of the ODMRP's forwarding group.

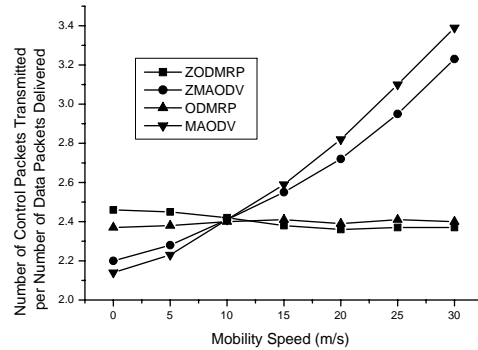


Figure 8: Number of control packets transmitted per Number of data packet delivered as a function of mobility speed

Finally, Figure 9 reports the results of the delivery ratio of useful data packets as a function of the multicast group size. We define useful packets as all those packets that reaches the destination first (all lost or duplicate data packets are not counted). A low ratio indicates good protocol performance. The results show that the performance of ZODMRP and ODMRP are almost the same, and lower than their MAODV counterparts. This is due to their multicast forwarding technique based on the mesh topology that generates a considerable number of useless (and redundant) data packets when the multicast group size is small. However, the performance improves rapidly with the increase of the multicast group size, and gets closer to the performance of the MAODV group for large sizes of the multicast group.

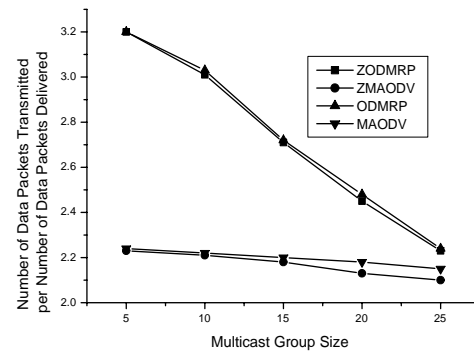


Fig. 9: Number of data packets transmitted per data packet received as a function of multicast group size

Concluding the analysis, we consider that the variants including the zone routing features are superior in providing QoS to the standard multicast routing

protocols, when connecting Ad-Hoc islands to infrastructure based networks and thus to the internet. The performance increase is especially visible when comparing ZMAODV with MAODV. However, when considering QoS provisioning under the aspect of terminal mobility, ZODMRP is the method of choice.

7 Conclusion

We have presented a proposal for the integration of Ad-Hoc islands with infrastructure-based networks for providing multicast operations for users across both domains. The proposed scheme has interesting applications in hotspots' design and extensions thereof. This approach enables a seamless integration of wireless MANs and LANs with the public Internet, providing a common multicast framework. We have proposed and evaluated two new hybrid protocols ZODMRP and ZMAODV (based on the ODMRP and MAODV protocols) that were built using the zone routing concept. Extensive simulations of these protocols, and their original counterparts, revealed the superiority of the ZODMRP in providing predictable QoS guarantees for multicast sessions.

Our future work concentrates on exploiting Ad-Hoc mechanisms inside the 802.16 network, especially in the case of mobile and meshed 802.16 networks and evaluating the overhead of the announcement of default routes for the Ad-Hoc nodes. With respect to multicast routing in Ad-Hoc networks connected to the internet, we are working towards more realistic mobility models applicable to public hotspot environments. We will evaluate then our approaches contrasting different mobility models (including random waypoint) and compare our approach with other multicast variants for Ad-Hoc networks. We will consider other performance metrics like the connectivity of clients, delay for a client to be connected to multicast sources located in the internet or Ad-Hoc fringe, or total bandwidth consumption. Also, we will extend our simulations to cover multiple access routers and deploy load balancing strategies. But this will require extensions of the routing protocol messages to carry such load information.

Acknowledgement

The work described in this paper is partly based on results of IST FP6 Integrated Project DAIDALOS. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. In addition, the work

by Pedro M. Ruiz has been funded by the "Ramon y Cajal" workprogramme of the Spanish Science Ministry.

References

- [1] IEEE 802.16-REVd/D2-2003, "IEEE Draft for Local and Metropolitan Area Networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems", November 2003.
- [2] Carl Eklund, Roger B. Marks, Kenneth L. Stanwood and Stanley Wang, "IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access", IEEE Communications Magazine, June 2002.
- [3] Development of the IEEE 802.16 WirelessMAN-ET Standard for Wireless Metropolitan Area Networks, accessible at <http://www.ieee802.org/16/tge/>
- [4] Fenner, W., Internet Group Management Protocol, Version 2. RFC 2236, November, 1997.
- [5] Estrin, D. et. al., "Protocol Independent Multicast Sparse Mode (PIM-SM): Protocol Specification." RFC 2362, June 1998.
- [6] E. Bommaiah, M. Liu, A. McAuley, R. Talpade, "Ad-Hoc Multicast Routing Protocol", Internetdraft, Aug. 1998.
- [7] C. Wu, Y. Tay, C. Toh, "Ad-Hoc Multicast Routing Protocol utilizing Increasing id-numbers (AMRIS): functional specification", Internet-draft, November 1998.
- [8] E.M. Royer and C.E. Perkins, "Multicast Ad-Hoc On-Demand Distance Vector (MAODV) Routing," Internet-Draft, draft-ietf-manet-maodv-00.txt, July 2000.
- [9] Yunjung Yi, Sung-Ju Lee, William Su, and Mario Gerla, "On-Demand Multicast Routing Protocol (ODMRP) for Ad-Hoc Networks," Internet-Draft, draft-yi-manet-odmrp-00.txt, March 2003
- [10] J. J. Garcia-Luna-Aceves and E.L. Madruga, "The Core-Assisted Mesh Protocol," IEEE JSAC, Aug. 1999, pp. 1380–94.
- [11] P. Sinha, R. Sivakumar, and V. Bharghavan, "MCEDAR: Multicast Core-Extraction Distributed Ad-Hoc Routing," IEEE Wireless Commun. and Net.Conf., Sept. 1999, pp. 1313–17.
- [12] Young-Bae Ko, Nitin Vaidya: "Geocasting in Mobile Ad-Hoc Networks: Location-Based Multicast Algorithms", Technical Report TR-98-018, Texas A&M University, September 1998.
- [13] C. Jelger, T. Noel: "Unicast and Multicast Gatewaying in IPv6 Ad-Hoc networks", SAFARI workshop 2004, https://safarirrt.rtd.francetelecom.com/Public/workshop_safari_2004/
- [14] W. Ding, "Multicast Routing in Fixed Infrastructure and Mobile Ad-Hoc Wireless Networks with a Multicast Gateway", Carleton University, Ontario, Canada, July 2002.
- [15] P. Ruiz et al., "The MMARP Protocol for Efficient Support of Standard IP Multicast Communications in Mobile Ad-Hoc Access Networks". In proc. of the IST Mobile & Wireless Comm. Summit 2003, June 2003.
- [16] GloMoSim: A Scalable Simulation Environment for Wireless and Wired Network Systems. <http://pcl.cs.ucla.edu/projects/glomosim/>.