Ubiquitous Access through the Integration of Mobile Ad-hoc Networks

S. Sargento[1], R. Sarrô[1], R. Duarte[2], P. Stupar[3], F. Gallera[4], M. Natkaniec[5], J.P. Vilela[6], J. Barros[6]

[1]Instituto de Telecomunicações, Univ. Aveiro, [2]INESC Porto, [3]Telecom Italia Lab, [4]Univ. of Murcia, [5]AGH Krakow, [61]Instituto de Telecomunicações, Univ. of Porto

***Abstract*—The increasing requirement for ubiquitous access of the users, enable the seamless support of different networks, with different technologies, and also with different types, such as moving networks and ad-hoc networks.**

This paper describes the Ad-hoc network integration architecture being developed inside the IST project Daidalos II. The main purpose of this architecture is to seamlessly support the movement of nodes between ad-hoc and infrastructure networks, maintaining in the ad-hoc networks all the features being supported in the infrastructure, such as, efficient routing for unicast and multicast flows, distributed QoS mechanisms, security, and seamless mobility, including multihoming support.

***Index Terms*—Ad-hoc networks, mobility, multihoming, IEEE 802.21, QoS, secure routing.**

I. Introduction

Daidalos II [1] is an EU IST research project that is working to define and validate the network architecture of future mobile operators. A key requirement for these networks is the support of ubiquitous access. With the current evolution of technologies we envision that, to provide this ubiquitous access, users will access to the services through a heterogeneous landscape of technologies, and through different types of networks, including mobile ad-hoc networks (MANET) and moving networks (NEMO).

Daidalos II is defining a network architecture to provide ubiquitous access integrating heterogeneous access networks and providing seamless movement among them. The architecture will also support the following features: (1) mobility management is splitted between local and global domains; (2) it explores an identity based mobility management solution through the independent and general management of identities; (3) it integrates MANETs and NEMOs in the mobility architecture; (4) host multihoming - the host owns multiple physical network interfaces and concurrently gets access through them; (5) integrates ubiquitous and pervasiveness concepts for customized services to the users.

This paper addresses the support of MANETs integration developed under the framework of Daidalos II. This architecture aims at seamlessly support nodes moving between infrastructure and ad-hoc networks, maintaining its access to the Internet with the same quality. For this purpose, the MANET needs to support routing integration, QoS support, security of routing, and mobility with multihoming support. The remainder of the paper is structured as follows. Section II presents the overall network architecture, while section III and IV present the routing and QoS support. Section V describes the secure routing, and section VI describes the mobility process, including the multihoming support. Finally, section VII presents our conclusions.

II. Network Architecture

The proposed architecture recognizes the current trend in networks to a heterogeneous landscape of access providers. In such environment it is important to give to access providers (e.g. ISP or NAP) the flexibility of managing users mobility inside their own domain without requiring an interaction with the global mobile operator domain. Thus, it is envisioned the splitting of mobility management into different levels: a global level associated with the mobile operator network and a local level associated to network access providers (see Figure 1). This view is in line with the current trends envisioned in the NetLMM IETF Working group [2] but a number of extensions are proposed, e.g.: support of heterogeneous (multi-technology) local domains, support of multihoming both at global and local domain, support and integration of MANETs and NEMOs clouds. Although, for simplicity, the architecture in Figure 1 restricts a local domain per technology or type of network, we consider that a local domain is an operator network that, eventually, may be heterogeneous and contain several technologies.

In the global domain, mobility is supported by means of a global mobility protocol (GMP), such as Mobile IPv6 (MIPv6) [3] or Host Identity Protocol (HIP) [4]. Terminal mobility within a local domain is handled via local mobility protocols (LMP), which are transparent to the core network and independent of the GMP. In this case, when a mobile node moves within a local domain, only the LMP used in that domain operates; when the node moves across domains, only GMP operates.

Terminals roaming across different access networks (ANs) potentially implementing different wireless/wired access technologies have therefore the possibility to receive/send data from/to different ANs, eventually at the same time. This opens a new variety of business opportunities where users can choose the most suitable technology depending on several parameters such as application requirements, user profiles or network conditions. Considering such complex environments

where the terminal might not have the chance to retrieve all the necessary information about neighbouring access points/wireless stations, the network is required to implement intelligent functions to manage information systems as well as mobility, resources and QoS. While these aspects are typically managed in separated ways in standard GSM/3G networks, beyond 3G platforms assume the IPv6 layer as a common convergence layer to handle both data plane and control plane. Thus, mobility, resource management and QoS cannot be regarded anymore as independent issues. The proposed architecture considers the IEEE 802.21 [5] framework as the "glue" to provide the required functionalities and associated signalling methods both in the network and in the terminal side. Thus, while traditional host based mobility will be maintained, more intelligent systems for network decision and network handover trigger are being investigated and developed.

Mobile terminals (MTs) equipped with multiple wireless access technologies enable the opportunity for multihoming. The control plane of such technology can be implemented at global level where the mobile operator owns the functionalities for multiple bindings or locally keeping this transparent outside the local domain. MTs can be therefore multihomed without the mobile operator knowing users' settings.

One of the Daidalos II key aspects is the virtual identity (VID) concept, which provides privacy to the entities utilising it. A user needs/wants to be able to remain anonymous to the service provider and to neighbouring users. Service providers need not know the preferences of any given user and, at the same time, they need sufficient information for charging and accounting. The VID framework provides the possibility to instantiate several virtual users (even being physically only one user), all potentially using the same or different physical devices. From the network perspective, VIDs behave as different users with different preferences.

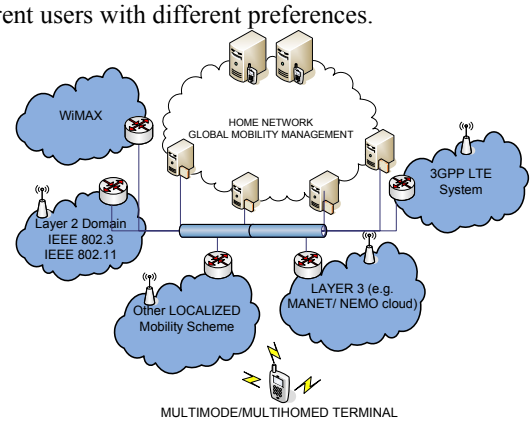

Figure 1 – Daidalos II network architecture

In this architecture, we consider local domains composed by MANETs and NEMOs, as shown in Figure 1. For both these networks, the concept of local/global mobility has large impact on the mobility between one of these networks and the infrastructure. The envisioned MANETs in Daidalos II are considered as multi-hop networks connected to the core network by means of one or more gateways. Therefore, since access clouds are considered as local mobility domains, the integration of MANET within the overall architecture requires the analysis of the interaction between these networks with the LMP. These interactions depend on the number of gateways supported and its location, in the same or different local domains. This has impact on the ad-hoc nodes address configuration and on the mobility management.

Finally, one of the most relevant tuning parameters to provide mobility decisions is the availability of information from the surrounding context. Ubiquitous and Pervasiveness (USP) are regarded here as a new set of triggers which the architecture can benefit from enabling more customized set of services such as mobility. In this view, terminal mobility and related handover control can receive triggers from network related conditions events as well as from less traditional triggers, such as context information (such as location information, network coverage).

The next sections describe how to support in ad-hoc clouds the same functionalities as the infrastructure: routing (unicast and multicast), QoS, security and mobility (with multihoming).

III. ROUTING

A. Unicast Routing

In order to better support multiple types of networks, both reactive and proactive routing protocols can be used in Daidalos II, namely AODV [6] and OLSR [7].

Supporting both these protocols simultaneously on the same MANET would not sum up the advantages of each protocol, also leading to excessive overheads caused by these protocols messages. The support of interoperability between clouds running OLSR and clouds running AODV seems complex from a control perspective; it would also require some nodes to provide the functionality to forward the packets between different clouds. These nodes would consume more power than normal nodes and have less processing power available for applications. These intermediate nodes would have to change very often if topology changes are frequent.

We decided to make all nodes and gateways support, if required, both OLSR and AODV, but enforcing the use of the same protocol in the same MANET. When the gateway decides to switch to a different routing protocol, its choice is advertised to all the nodes in the MANET. When a node receives a request to change protocol, it enables the new routing protocol and disables the previous.

The decision of what routing protocol to use in real-time is a research topic being addressed. The gateway has to gather information about the MANET density, the nodes mobility, the characteristics of the nodes, and the characteristics of the active flows. The gathering of this information demands new messages or a novel mechanism which infers a metric from the information made available by the routing and auto-configuration protocols. While such mechanism is not available, the choice is administrative; in a Stadium, for instance, OLSR is selected when a game is taking place and the stadium full, and AODV otherwise.

The support of efficient localized mobility demands also optimizations. The architecture has to support nodes coming from other networks which will maintain their prefix. This

node needs to flood a request to every address, even if from a different network prefix. In order to enhance performance, the gateway sends a Route Reply every time the destination node is not registered with it. OLSR can work unchanged in this scenario, given that the packets are sent to the gateway every time the destination does not figure on the local routing table.

The privacy requirements of VIDs imply the use of virtual interfaces (one for each physical interface available to each VID). In the MANET architecture, the virtual terminal will be characterized by a Virtual MAC (VMAC), Care-of-Address (CoA) and routing protocol; each VID runs its routing protocol instance, with its additional addresses.

B. *Multicast Routing*

Similarly to Daidalos I, MMARP (Multicast MAnet Routing Protocol) [8] has been chosen to provide MANET multicast routing in Daidalos II due to two reasons: MMARP provides efficient multicast routing inside the MANET, and it is specially designed for interoperate with multicast-enabled gateways which are placed in the access network. The MMARP protocol has been enhanced with new routing metrics and adapted to the network architecture based on LMDs.

1) *Enhanced routing metrics for MMARP*

A wireless routing algorithm can select better paths by explicitly taking the quality of the wireless links into account. The routing metric selected to improve the MMARP performance is based on the Expected Transmission Count (ETX) [9] metric which minimizes the expected total number of packet transmissions (including retransmissions) required to successfully deliver a packet to the ultimate destination. The original ETX metric assumes that a sender will retransmit a packet that is not successfully acknowledged. This is the case of unicast transmissions, but multicast and broadcast transmissions do not use the 802.11 ARQ mechanisms, so we have redefined the ETX metric to adapt it to a multicast protocol such as MMARP.

2) *MANET multicast routing integration in LDMs*

MMARP uses the Multicast Listener Discovery (MLD) protocol [10] as a means to interoperate with the multicast-enabled gateways. This mechanism also allows MMARP to be integrated in the LMD architecture. The MAG nodes must be multicast-enabled routers which allow multicast packets to be received on the interface of the MANET by successfully passing any Reverse Path Forwarding (RPF) check. MMARP nodes will use the MAG they are attached to establish multicast communication with nodes attached to a different MAG.

IV. QoS

Ad-hoc and infrastructure networks need to be closely integrated to provide the adequate service delivery and support of differentiated QoS in an integrated way for the users and services. The proposed QoS approach is based on an extension of the Stateless Wireless Ad-hoc Networks (SWAN) [11] QoS model, and abstracts the ad-hoc path between an ad-hoc node and the gateway as a virtual link in the infrastructure side [12].

The IEEE 802.11e standard with MAC layer QoS support is used to perform L2 service differentiation as it implements four different hardware queues. IEEE 802.11e standard supports EDCA (Enhanced DCF Channel Access) which opens various parameters for service differentiation configuration, namely: CW_{min}, CW_{max}, AIFS, and TXOP. The EDCA is designed to provide differentiated, distributed channel accesses for frames with different priorities. It is recommended to always use RTS/CTS frames exchange before the data transmission to minimize the negative effect of hidden stations.

The gateway QoS stack is able to support the same functionalities as the mobile nodes, but does not have interaction with the application signaling. Instead, it needs to perform interoperation between the QoS signaling in the ad-hoc and the infrastructure side. The service differentiation model is shown in Figure 2.

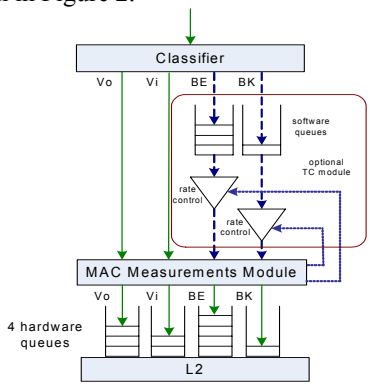

Figure 2 – Ad-hoc service differentiation model

Daidalos II L2 service differentiation can speed up the service differentiation process and allow simplifying Daidalos I architecture [12]. This enhanced type of service differentiation assumes four traffic classes, i.e., conversational real-time services, streaming real-time services, interactive best effort and background best effort. Every node requesting a service at session setup time can send a request for bandwidth allocation. Such request can be later dynamically adjusted thanks to feedback from L2 (MAC layer measurements). The traffic control module in Daidalos II is optional and can be removed if only L2 service differentiation is sufficient; if not, shapers can be used only for the two lower priority classes (as shaping of the real-time streams, such as voice and video, is unacceptable in most cases). In this case, it seems more reasonable to renegotiate a new (lower) transmission rate (i.e., choose another voice or video codec type) for these real-time streams or simply, to discard all new requests if the overload of the per-class available bandwidth within these high priority classes is observed.

V. Secure Routing

Due to the distributed nature of MANETs, the success of their network operations is greatly dependent on the level of cooperation between the involved entities. This requirement is particularly prominent with respect to the discovery and establishment of routes for reliable and secured data delivery. Motivated by this observation, we provided security

extensions for both the AODV and the OLSR standard MANET routing protocols.

SAODV [13] is an extension to the AODV protocol that protects routing information and the route discovery mechanism, providing features such as integrity, authentication and non-repudiation. SAODV, which is based on public-key cryptography, uses digital signatures to ensure the authenticity of the messages, and a Lamport hash chain to protect the nodes from misusing the protocol and to force sub-optimal routes.

Cooperative Security Scheme (CSS)-OLSR [14] is an extension to the OLSR protocol that secures the routing protocol by rewarding users that comply with the routing protocol and penalizing damaging behaviour. For this purpose, two new elements are added to the regular OLSR operation:

- *Complete Path Message (CPM)*: a CPM is used to convey the path traversed by control traffic messages which are flooded by OLSR throughout the network. A CPM is sent back, accordingly to the defined CPM rate, by the recipient of a control traffic message containing the path traversed by that message;
- *Rating Table*: each user of the network keeps a rating table which holds information about the behaviour of other users. Each entry in the rating table has a user ID, a primary and secondary ratings. The secondary rating is a classification of the user based on direct observation of retransmissions, while the primary rating is a more mature classification based on the correlation of the secondary rating, the information provided by the CPMs and the local routing information kept by the devices.

CSS-OLSR features a set of mechanisms for misbehaviour detection based on the analysis of retransmissions (similar to the *watchdog* concept [15]), and for the detection of fake control traffic. The key here is to exploit the correlation between the local routing information and the data provided by the CPMs. Both these mechanisms lead to changes in the primary and secondary ratings of each user, which are then used to punish those that are misbehaving users, e.g. by reducing the willingness to perform routing operations on their behalf.

VI. Mobility

A. IEEE 802.21 and Local Mobility

The IEEE 802.21 Media Independent Handover (MIH) services [5] is a working draft in development in the IEEE that aims to provide an 802 independent mechanism to perform handover between heterogeneous 802 systems, and between 802 systems and cellular systems. The great advantage of this protocol is that it provides a standard way of performing the signal and control of the handover process independently of the 802 technologies being used underneath. The 802.21 MIH protocol requires that an abstraction layer is added between the 802 drivers and the upper layers, in order to provide the desired technology independency; this layer is called MIH Function (MIHF). The MIHF receives events and information from the drivers and processes it before sending it to the upper layers; the MIHF also represents the entity responsible for controlling and signal the handover process.

The advantages of the 802.21 protocol comprise the gained independency in the technology chosen, and thus seamlessly support of all 802 technologies, and the fact that it provides to the nodes and the network a generic way to detect events that have occurred in the terminal itself, as well as in the network.

A problem exists, however, with the way the 802.21 information (commands, information and events) is exchanged between the terminal (MT) and the point of access to the network (PoA). The 802.21 is created for infrastructure networks, in where the MN and the PoA are always one link away from each other, which is not true in ad-hoc networks. The solution found to solve this issue is to expose the MANET as a new technology to the MIHF, this technology does only support L3 messages, and this solution guarantees that the MIHF will be capable of sending and receiving from the network the necessary messages.

Another problem concerns the events, generated by the 802.21 Event Service that flows from the technology driver to the MIHF inside the MT. In the standard form, all events generated by the driver are sent to the MIHF, but as the MANET is now presented as an L3 technology, these L2 events are not meaningful. Only the events generated based on L3 information (like route errors from the routing protocols or lost connectivity with the gateway from the auto-configuration protocol) are useful for the decision taking logic and the handover controlling modules. A new module is added to the architecture of the terminal, between the driver and the MIHF. This module, the MANET Wrapper, has the responsibility to generate the 802.21 events from the L3, using information from the routing protocols and auto-configuration, emulating a virtual link (with one hop) between the MT and the gateway.

Once the correct support for the 802.21 MIH protocol is in place, the messages for handovers request and reply can be also used to transmit QoS parameters so that, upon handover, the QoS sessions can be maintained with the same quality. The local mobility itself is done recurring to a network based mobility protocol, similar to the one in development in the Netlmm IETF WG,[2].

The adaptation needed for the MANET to work in a LMD relates to the gateway's ability to detect the nodes movement, This can only be done if the MT explicitly notifies the gateway about its new location; therefore, when a terminal arrives to a new network, it signals the gateway so that the local mobility protocol can be triggered. This solution accomplishes two purposes: the movement detection by the local mobility protocol, and the start of the bootstrapping procedure, described in the next section.

B. Bootstrapping process

Bootstrapping is the process by which the MT gets the necessary information needed to have full access to the network. In a typical infrastructure network, the MT is always one link away from its point of attachment, and thus can communicate directly with it. This communication is easily done by using IPv6 link-layer addresses and Layer 2 messages. Unlike in the infrastructure, direct communication between ad-hoc nodes and the gateway may not be possible; in this scenario, Layer 3 communication needs to be in place between the node and the gateway. However, considering that

the communication is performed to the outside, this requires that a globally scoped IPv6 address is configured on the network card. Unfortunately, a globally scoped MT address is only available after the bootstrap phase, so, some other temporary address must be used instead. For this operation, we decided to use the Unique Local IPv6 Unicast Addresses (ULA) [16]. These addresses replace the link-layer addresses for operations inside the MANET.

During the bootstrap phase, the node should only have access to the PoA, and should not be part of the routing protocol operations, because it is not fully authorized to use the network. The gateways should also drop packets proceeding from Local IPv6 Unicast addresses. With a unique local unicast address, the node is only allowed to have bi-directional connectivity to the gateway. The bootstrap operation consists on the MT sending its credentials, and then the gateway sending the prefix assigned to it.

The knowledge of the gateway and its address is given by the Jelger auto-configuration protocol [17], which spreads the information in the network, and builds a tree with all nodes in the network (any node can reach the gateway through simple forwarding).

To enhance performance, limit the access to the network and minimize the awareness of the entrance of a new node, a simplification of a routing protocol such as AODV can be used. A node entering the network generates its address through auto-configuration and sends a Route Reply, addressed to the gateway, reachable using the path created by gateway discovery. This message creates a temporary bi-directional link between the node and the gateway. The gateway then communicates with the network and verifies if the node is allowed to use it. In case the node is authorized, the gateway sends the prefix assigned by the network to the node's unicast local address. The node generates a valid global address, based on the received prefix, and starts the fully functional ad-hoc routing protocol.

C. Mobility Execution

In Daidalos II the 802.21 MIH framework is used to manage mobility in the architecture, across all access technologies. To fully explore the MIH functionality in MANET, as discussed in section VI.A, it is desirable that the ad-hoc network is presented to the MIH Layer as a different technology, even if the real technology used is 802.11. To do so, the MIH-LINK-SAP (Service Access Point) abstract interface must be implemented by the ad-hoc modules, using not only information and operations provided by ad-hoc auto-configuration and routing protocols, but also from the 802.11 L2 events provided by the driver. Because the same card can be used for infrastructure and ad-hoc connectivity, our MANET module presented to MIHF must keep the 802.11 functionalities of the original 802.11 module (WLAN-RAL), and extending it with the MANET information.

To transparently use the same module in ad-hoc and infrastructure mode, we introduce a wrapper between WLAN-RAL and the MIHF. The wrapper communicates with both 802.11 RAL and ad-hoc modules, and generates meaningful messages to the MIH. The events are processed by MANET wrapper in a way that they have relevance in the context of the MANET. Commands from the MIHF can trigger operations on the MANET modules and on the 802.11 RAL as well.

MIH manages a collection of information regarding available PoA for each technology. As an example, 802.11 infrastructure PoAs are 802.11 APs. An 802.11 PoA is available when a node is inside the PoA wireless range. The link quality to that PoA can be characterized using the signal strength metric. MANET wrapper introduces the ad-hoc PoAs to the framework: ad-hoc PoAs are the ad-hoc gateways with connection to the infrastructure. We call this path inside the MANET that enables a node to reach the gateway an ad-hoc Virtual Link. The metrics that characterize the quality of the PoA will relate to the virtual link. For example, a PoA can be selected instead of another because the virtual link towards it has a smaller hop count than the other. Information about the Virtual Links are provided by an information protocol similar to Daidalos I auto-configuration, that inform a MT about the reachability of a gateway, and provide a metric that characterizes the path to it, that is updated hop-by-hop.

MANET is supported at a lower level inside the MIH architecture, and the MIH-Users (eg: handover controllers) will interact with the MANET using the abstract interface they use for the other technologies. They still have to be MANET aware, so that they can take decisions on what PoA to use and implement policies.

By introducing the wrapper, the ad-hoc handover operations are managed in a seamless way as to the infrastructure.

D. Multihoming

Ad-hoc networks are characterized by unpredictable topologies determined by nodes' mobility degree. Indeed it may happen that a MANET is connected to an external network by means of several gateways, i.e. a node can exploit several ingress/egress points to exchange traffic with hosts located outside the MANET it is connected to. The plurality of gateways can be exploited to achieve redundancy and load balancing. Redundancy is an inherent feature of multiple gateways MANET but attention must be paid to the operations executed to replace or change the gateway. The considered approach is the enhancement of routing protocols proactively announcing topology information: nodes periodically transmit OLSR MID messages containing all the usable global addresses; if AODV is used, a Gratuitous Route Reply is sent to each gateway with the global address associated to the gateway itself. When the node changes the gateway used to exchange packets, the MANET already knows the required routing information to deliver packets destined to the node. Load balancing is achieved by endowing the MT of a gateway selection engine which assigns flows to the proper gateway. Such engine has to consider as inputs the distance of the gateways from the hop. This is the main difference with a load balancing method used in host-multihoming in infrastructure-based networks. Since session maintenance is a fundamental requirement nowadays, multihoming in MANET is fitted within mobility infrastructure, both global and local. Global mobility copes with multihoming when different gateways announce different prefixes: this implies that a node can use several CoAs to communicate. All the set of available

addresses have to be registered with the mobility anchor, e.g. Home Agent in case MIP is used. MIPv6 framework will be extended with multiple CoAs (bound with the same HoA) support and will be MANET unaware (i.e. Binding Updates messages are the same as those used for standard MIPv6 multiple registration). Policy management handling distribution of flows among available gateway is performed by using flow identifier extensions of MIPv6: each flow is identified by a 5-uple (IP source address, IP destination address, source port, destination port and protocol type); such 5-uple is identified by a Flow ID (FID) which is communicated to home agent or correspondent node if route optimization is performed. FIDs are then bound with CoAs associated to the gateway through which that particular flow has to be exchanged: data packets of a specific flow will be transmitted to the CoA bound to that flow and therefore will be routed to the gateway announcing the prefix of that CoA. OLSR MID messages and AODV Gratuitous Replies cope with the set-up of routing information to deliver packets destined to the CoAs of the node. Uplink traffic distribution is achieved by means of IPv6 routing header. Indeed, routing in ad-hoc networks is performed in a hop-by-hop manner; therefore, a node wishing a certain flow to be sent through a chosen gateway has to insert a routing header and put as the first destination the address of the chosen gateway.

If multihoming is performed at LMD level some additional extensions have to be provided. Indeed a node connected to multiple gateways belonging to the same LMD will receive only one prefix which will be handled by all the gateways. This implies that an additional data is required to handle downlink packets distribution. The proposed solution exploits FID used by MIPv6 to identify flows for routing purposes. If it has been established that a certain flow has to be exchanged to a gateway A, then the node communicates the FID of the flow to gateway A by using 802.21 messages. Gateway A, in turn, registers the triple made by such FID, node CoA and gateway identifier with LMA through NETLMM extended messages. Our solution requires the insertion of FIDs into the IPv6 Flow label field of outer IPv6 header of packets transmitted to the node: such operation is executed by home agent or correspondent node (when route optimization is run). LMA will then receive packets destined to the CoA of the node and labeled with a specific FID: it will perform a lookup in its extended routing table by examining CoA and FID and will find the gateway to which the packet (and hence the flow the packet belongs to) has to be delivered. MANET routing will handle packet transmission from gateway to the node.

It may happen that multihoming within a MANET has to be handled both by LMP and GMP. Indeed it may happen that a MANET is endowed with multiple gateways which can be split into multiple subsets of gateways belonging to the same LMD. This scenario implies a hierarchical approach: multihoming at GMD level handles distribution of flows among the subsets of gateway belonging to the same LMD, and multihoming at LMD level controls the delivery of the traffic to the chosen gateway. No changes to the previously described approaches have to be performed.

VII. Conclusion

This paper described the Ad-hoc network integration architecture being developed inside the IST project Daidalos II, mainly in terms of its functionalities and interactions to efficiently support the delivery of diversified services to users connected to the ad-hoc network. The proposed architecture is able to efficiently integrate ad-hoc and infrastructure networks, enabling a node to be using one of the networks or both (through multihoming), and to seamless move between ad-hoc and infrastructure networks. The ad-hoc architecture is designed in such a way that the mobility process is independent of the type of network in place. Beyond seamless mobility, the support of unicast and multicast routing, distributed QoS and secure routing, are also in place.

Acknowledgment - The work described in this paper is based on results of IST FP6 Integrated Project Daidalos II. The authors wish to thank the partners of the Daidalos II Consortium, in particular partners of WP2.4, for their collaborative work.

References

[1] IST FP6 Integrated Project Daidalos II: http://www.ist-daidalos.org.
[2] J. Kempf, et al, “Goals for Network-based Localized Mobility Management (NETLMM)”, draft-ietf-netlmm-nohosts-req-03, 2006.
[3] D. Johnson, C. Perkins, J. Arkko. Mobility Support in IPv6, IEFT RFC 2775, June 2004.
[4] R. Moskowitz, et al, “Host Identity Protocol”, draft-ietf-hip-base-06, June 2006.
[5] Draft Standard for Local and Metropolitan Area Networks: Media Independent Handovers Services (Draft .01). IEEE, March 2006.
[6] C. Perkins et al., “Ad hoc On-Demand Distance Vector (AODV) Routing”, IETF experimental RFC 3561, July 2003
[7] T. Clausen, P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, IETF experimental RFC 3626, October 2003.
[8] 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.
[9] D. Couto et al., “A high-throughput path metric for multi-hop wireless networks”. In *MobiCom* 03, Sept 2003.
[10] S. Deering, W Fenner, B. Haberman., “Multicast Listener Discovery (MLD) for IPv6”, IETF RFC 2710, October 1999
[11] G.-S. Ahn et al., “Supporting Service Differentiation for Real Time and Best-Effort Traffic in Stateless Wireless Ad Hoc Networks”. IEEE Trans. on Mob. Comp. vol. 1, no. 3, 2002.
[12] S. Crisóstomo, S. Sargento et al., *A QoS Architecture Integrating Mobile Ad-Hoc and Infrastructure Networks*, 3rd ACS IEEE Int. Conf. on Computer Systems and Applications AICCSA’05, 2005.
[13] M. Zapata, “Secure Ad hoc On-demand Distance Vector (SAODV) Routing”, IETF Internet-Draft: draftguerrero-manet-saodv-00.txt, 2001.
[14] J. P. Vilela and J. Barros, "A Cooperative Security Scheme for Optimized Link State Routing in Mobile Ad-hoc Networks". Proc. of the 15th IST Mobile and Wireless Comm. Summit, June 2006.
[15] S. Marti et al., “Mitigating routing misbehavior in mobile ad hoc networks”. In Proc. of MOBICOM 2000, (August 2000).
[16] R. Hinden, B. Haberman., “Unique Local IPv6 Unicast Address”, IETF RFC 4193, October 2005.
[17] C. Jelger, T. Noel, ”Gateway and address autoconfiguration for IPv6 adhoc networks”, IETF Internet Draft, draft-jelger-manet-gateway-autoconf-v6-02.txt, April 2004.