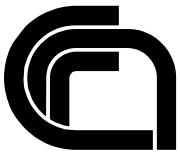

Consiglio Nazionale delle Ricerche

A MobileMAN Approach for the Interconnection of Heterogeneous Ad Hoc Networks to the Internet

E. Ancillotti, R. Bruno, M. Conti, E. Gregori and A. Pinizzotto

IIT TR-08/2010

Technical report

Febbraio 2010

Istituto di Informatica e Telematica

A MobileMAN Approach for the Interconnection of Heterogeneous Ad Hoc Networks to the Internet

Emilio Ancillotti*, Raffaele Bruno†, Marco Conti†, Enrico Gregori† and Antonio Pinizzotto†
*Dept. of Information Engineering, University of Pisa
Via Diotisalvi 2 - 56122 Pisa, Italy
Email: emilio.ancillotti@iet.unipi.it
†IIT Institute, National Research Council (CNR)
Via G. Moruzzi, 1 - 56124 Pisa, Italy
Email: {r.bruno,m.conti,e.gregori,a.pinizzotto}@iit.cnr.it

Abstract

The recent advances in mobile and ubiquitous computing, and the development of inexpensive, portable devices are extending the application fields of ad hoc networking far beyond the traditional view of *stand-alone* networks. Indeed, it is now recognized that a prerequisite for the commercial penetration of the ad hoc networking technologies is an easy access to the Internet and its services, and their integration into traditional wired/wireless infrastructure-based networks. In this chapter we review the different approaches that have been proposed to provide Internet connectivity for ad hoc networks, pointing out advantages and drawbacks of each of them. Possible strategies are to implement an extended Mobile IP Foreign Agent (MIP-FA) or a Network Address Translation (NAT) in the gateway interconnecting the ad hoc network with the external Internet. However, these solutions are based on complex IP-based mechanisms originally designed for the wired Internet. In this chapter we also describe an alternative approach, in which basic layer-2 functionalities are exploited to build a multi-hop heterogeneous (i.e., using wireless and wired links) proactive ad hoc network that could be used as a flexible and low-cost extension of traditional wired LANs. This architecture is validated by an implementation based on the OLSR protocol developed in the framework of the MobileMAN Project.

I. Introduction

A mobile ad hoc network (MANET) is a collection of mobile nodes connected together over a wireless medium, which self-organize into an autonomous multi-hop wireless network. Traditionally, MANETs have been considered as small-scale *stand-alone* networks, i.e., self-organized groups of nodes that operate in isolation in an area where deploying a networking infrastructure is not feasible due to practical or cost constraints (e.g., disaster areas, battlefields, temporary networks, etc.). However, the recent advances in mobile and ubiquitous computing, and the development of inexpensive, portable devices are further extending the application fields of ad hoc networking. For instance, the MobileMAN Project [1] has extensively investigated the key challenges of implementing ad hoc networks in medium to large-scale environments, such as metropolitan areas. The technical and sociological investigations carried out in the framework of this project have identified in the ability to support of an easy access to the Internet and its services one of the most important features capable of fostering the commercial penetration of the ad hoc networking technologies. Indeed, it is now extensively recognized that users are looking for multi-purpose networking platforms in which cost is an issue and Internet access is a must. As a consequence, nowadays,

multi-hop ad hoc networks do not appear as isolate self-configured networks, but rather emerge as a flexible and low-cost extension of wired infrastructure networks, coexisting with them. A new class of networks is emerging from this view, in which a mix of fixed and mobile nodes interconnected via heterogeneous (wireless and wired) links forms a multi-hop heterogeneous ad hoc network integrated into classical wired/wireless infrastructure-based networks [2].

In this chapter, we concentrate on investigating how this networking paradigm can be applied to extend the range of traditional Wireless Local Area Networks (WLANs) [3] over multiple radio hops, in order to provide seamless and untethered mobility support for mobile/portables devices in the local area environment. Ensuring a seamless coverage when deploying traditional infrastructure-based WLANs is a difficult challenge to address, because of the several factors that impair the radio transmissions, such as electromagnetic interference, fading, obstacles, etc. Integrating ad hoc networking in traditional WLAN technologies allows discovering and maintaining multi-hop wireless paths within the network, providing a flexible, robust and cost-effective solution to increase coverage areas. More precisely, we envisage a heterogeneous network environment in which wired and multi-hop wireless technologies transparently coexist and interoperate. In this network, separated group of nodes without a direct access to the networking infrastructure form *ad hoc "islands"*, establishing multi-hop wireless links. Special nodes, hereafter indicated as *gateways*, having both wired and wireless interfaces, are used to build a wired backbone interconnecting separated ad hoc components. In addition, the gateways use their wired interfaces also to communicate with static hosts belonging to a wired LAN. The network resulting from the integration of the ad hoc network with the wired LAN is an *extended* LAN, in which static and mobile hosts transparently communicate using traditional wired technologies or ad hoc networking technologies. Note that a similar architecture has been adopted in previous work dealing with connecting ad hoc networks to the Internet, such as [4]–[6].

A variety of architectural issues arise to offer IP basic services, such as routing and Internet connectivity, in this extended LAN. First of all, in the traditional view of ad hoc networks, no specific assumption is made about the IP addresses of mobile nodes. This means that each IP address serves only as a node's identifier and it does not convey any information about where the node is topologically located with respect to another node. As a consequence, routing in ad hoc networks is typically performed using only host specific routes. On the other hand, traditional IP routing is hierarchical and based on aggregated routes: one entry in the routing table can handle all the hosts that share the same network identifier. Thus, specific mechanisms are needed to enable mobile nodes to distinguish between IP addresses belonging to the ad hoc components or the wired part of this extended WLAN. Another problem that arises when providing ad hoc nodes with connectivity to external networks is how to allow that the return traffic is correctly routed from the rest of the Internet to the ad hoc source node. In addition to these general issues, there are other problems more related to the management of node mobility in terms of roaming between the different ad hoc components. Some kind of signalling is needed to detect the different available gateways, to select one of them and to handoff to a new gateway when appropriate.

In this chapter we aim at outlining the most relevant proposals presented in the literature to support Internet

connectivity in ad hoc networks. We will show that at least two different approaches can be identified when connecting ad hoc networks to the Internet. One approach requires that a Mobile IP Foreign Agent (MIP-FA) [7] module is implemented in one or more gateways. Ad hoc nodes that want Internet access should obtain in some way a care-of-address from the foreign agents and register it with their home agent. An alternative approach is to implement a Network Address Translator (NAT) [8] module in one or more gateways such as to allocate an IP address for external communications to ad hoc nodes that want to send packets to the Internet. Both of these approaches have been applied to different ad hoc routing protocols, and a variety of working solutions to the aforementioned problems have been proposed. However, as we will discuss in this chapter, these schemes have still a number of drawbacks because they usually rely on complex IP-based mechanisms originally defined for the wired Internet, like IP-in-IP encapsulation and IP tunnelling, which may introduce significant overheads and limitations. To overcome some of these limitations, in this chapter we present a novel architecture that exploits only *layer-2* mechanisms such as the ARP protocol, to logically extend the wired LAN to the ad hoc nodes in a way that is transparent for the wired nodes. By positioning our architecture at layer 2 (the data link layer), we may avoid undesired and complex interactions with the IP protocol and provide global Internet connectivity in a very straightforward manner. In addition, we also describe how dynamic address auto-configuration of the ad hoc nodes can be accomplished by using DHCP servers located in the wired part of the network. Using our scheme, mobile nodes can obtain a unique IP address that is topologically correct within the extended LAN. This architecture is validated by an implementation based on the OLSR protocol.

It is worth noting that recently other schemes have been proposed to provide ad hoc support below the IP layer. For example, in [9] label switching was employed to put routing logic inside the wireless network card. More recently, the LUNAR [10] ad hoc routing framework and the Mesh Connectivity Layer (MCL) [11] have been proposed. These solutions locate the ad hoc support between the data link layer and the network layer. This "Layer 2.5" is based on *virtual* interfaces that allow abstracting the ad hoc protocols from both the specific hardware components and network protocols. However, this interconnection layer requires its own naming and addressing functionalities distinct from the layer-2 addresses of the underlying physical devices. This may significantly increase the packet header overheads. On the contrary, our proposed architecture is totally located inside layer 2, reducing implementation complexity and ensuring minimal additional overheads.

The remainder of this chapter is organized as follows. Section II gives a brief introduction on the typical characteristics and functionalities of ad hoc routing protocols. Section III reviews solutions adopting MIP-FA based gateways, while Section IV outlines proposals integrating NAT-based gateways. The design principles and the operation details of the layer-2 architecture we propose to build heterogeneous ad hoc networks interconnected to the Internet are described in Section V. Section VI presents experimental results evaluating the throughput performance of Internet access. Finally, Section VII draws concluding remarks.

II. Routing in a MANET Network

In the traditional view of MANETs, these are collections of mobile nodes connected together over a wireless medium, forming a dynamic, multi-hop, self-organized and autonomous network. This means that we cannot assume that there is direct link-layer connectivity between nodes, but each node operates as a router forwarding packets for other mobile nodes in the network that may not be within direct wireless transmission range of each other. For these reasons, all the nodes in the ad hoc network must be provided with specific routing capabilities that allow them to discover multi-hop paths through the network to reach any designated destination.

A wide variety of routing protocols have been proposed by the MANET working group of the IETF [12]. These protocols can be divided into three main categories: reactive, proactive and hybrid [13]. Reactive protocols set up routes on-demand, i.e., when a node wants to initiate a communication with a node to which it has no route. In addition, such protocols maintain these routes only as long as they are needed by the sources. Generally, on-demand routing algorithms operate by flooding the network with special packets intended to discover a route between the source node and the designated destination. Examples of reactive protocols are the Dynamic Source Routing (DSR) protocol [14] and the Ad hoc On-Demand Distance Vector (AODV) protocol [15]. On the contrary, with proactive routing protocols each node continuously updates its topology information such as to have, ideally, a complete knowledge of the entire network. This results in a constant overhead generated by routing traffic, but a communication is not affected by the initial delay required to establish a new route, which typically occurs for on-demand routing algorithms. Examples of this type of protocols are the Optimized Link State Routing (OLSR) [16], and the Topology Dissemination Based on Reverse-Path Forwarding (TBRPF) [17]. Finally, the third category of routing protocols for MANETs consists of hybrid protocols that try to combine the proactive and reactive approaches. An example of such a protocol is the Zone Routing Protocol (ZRP) [18]. In particular, ZRP divides the topology into zones and utilizes different routing protocols within and between the zones, taking advantage of proactive discovery within a node's local neighborhood, and using a reactive protocol for communication between these neighborhoods.

The characteristics of the routing protocols for ad hoc networks, such as the fact that they operate without any centralized control or configuration, using primarily host specific routes along multi hop paths, and non-hierarchical addressing schemes, differ substantially from those of the fixed Internet and the standard IP routing. Thus, several issues arise when trying to apply IP-based mechanisms originally devised for the fixed Internet, such as Mobile IP, to the ad hoc networking. Consequently, the solutions proposed to provide Internet connectivity to MANETs have to take into account the basic design principles adopted in the underlying ad hoc routing protocol. To better understand the implications of multi-hop communications and ad hoc routing on the schemes implemented to ensure transparent Internet access to ad hoc nodes, in the following we give a short description of two of the most popular routing protocols used in ad hoc networks, one belonging to the category of reactive protocols (AODV) and the other one adopting a proactive approach (OLSR).

A. AODV

AODV [15] is a distance vector routing protocols that operates in an on-demand fashion. A node keeps track of its neighbors by listening for HELLO messages that each node broadcasts at periodic intervals, or by using feedback from the link-layer upon unsuccessful transmissions. When a source node desires to communicate with another node that is not its neighbor and for which it does not already have a valid route, it broadcasts a ROUTE REQUEST (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up a *reverse route entry* for the source node in the routing tables. In addition to the source node's IP address, current sequence number, and broadcast ID, the RREQ also contains the most recent sequence number for the destination of which the source node is aware. A node receiving the RREQ may send a ROUTE REPLY (RREP) message if it is either the designated destination or if it has a route to the destination with corresponding sequence number greater than or equal to that contained in the RREQ. If this is the case, it unicasts a RREP back to the source on the reverse route that was created by the RREQ message. Otherwise, it rebroadcasts the RREQ message to its set of neighbors. In other words, AODV uses sequence numbers to determine freshness of routing information, thus preventing routing loops. Nodes keep track of the RREQ's source IP address and broadcast ID, which uniquely identify a RREQ. If they receive a RREQ that they have already processed, they discard the RREQ and do not forward it.

As the RREP propagates back to the source, nodes set up *forward route entries* for to the destination in the route tables. Once the source node receives the RREP, it may begin to forward data packets to the destination. If the source later receives a RREP containing a greater sequence number or it contains the same sequence number with a smaller hop-count, it may update its routing information for that destination and begin using the better route. As long as the route remains active, it will continue to be maintained. A route is considered active as long as there are data packets travelling from the source to the destination along that path. Once the source stops sending data packets, the links will time out and eventually be deleted from the intermediate node routing tables. If a link break occurs for the next hop of an active route, the node invalidates all its routes utilizing than link. In addition, it creates a ROUTE ERROR (RERR) message containing the list of all the now unreachable destinations, i.e., the unreachable neighbor and any additional destinations in the local routing table that use the unreachable neighbor as the next hop. The node then broadcasts the RERR message to its neighbors. After receiving the RERR message, if the source node still desires the route, it can reinitiate a route discovery process.

B. OLSR

The OLSR protocol [16] is an optimization of the classical link state algorithm tailored to mobile ad hoc networks. More precisely, being a proactive routing protocol, OLSR periodically floods the network with route information, so that each node can locally build a routing table containing the complete information of routes to all the nodes in the ad hoc network running on their interfaces the OLSR protocol. The OLSR routing algorithm employs an efficient dissemination of the network topology information by selecting special nodes, the *multipoint relays* (MPRs), to forward broadcast messages during the flooding process. More precisely, each node independently selects its

multipoint relays among its one-hop neighbors such as to ensure that a broadcast message, retransmitted by these selected neighbors, will be received by all its two-hop neighbors. The link state reports, which are generated periodically by MPRs, are called TOPOLOGY CONTROL (TC) messages. These TC messages are flooded to all the nodes in the network, but only the MPRs are allowed to forward the control messages received from other nodes, in order to reduce the number of retransmissions needed to cover the entire network.

Similarly to the AODV protocol, OLSR employs a neighbor discovery procedure based on HELLO messages. These HELLO packets contain the list of neighbors known to the node and their link status. Thus, HELLO messages allow each ode to discover its one-hop neighbors, as well as its two-hop neighbors, which are needed during the MPR selection procedure. The neighborhood information and the topology information are updated periodically, and they enable each node to locally compute the least-cost routes to any possible destination in the ad hoc network, by using the Dijkstra's shortest path algorithm. This routing table is recomputed whenever there is a change in either the neighborhood information or the topology information.

In order to enable the injection of external routing information into the ad hoc network, the OLSR protocol defines the HOST AND NETWORK ASSOCIATION (HNA) message. The HNA message binds a set of network prefixes to the IP address of the node attached to the external networks, i.e., the gateway node. In this way, each ad hoc node is informed about the network address and netmask of the network that is reachable through each gateway. In other words, the OLSR protocol exploits the mechanism of *default routes* to advertise Internet connectivity. For instance, a gateway that advertises the $0.0.0.0/0$ default route, will receive each packet destined to IP addresses without a known route on the local ad hoc network.

III. INTERNET CONNECTIVITY USING MOBILE IP

One of the possible approaches to provide Internet connectivity for ad hoc networks is based on the integration of Mobile IP [7] with ad hoc routing protocols. In this section we give a brief description on the Mobile IP protocol, and then we outline different solutions proposed to connect an ad hoc network to the Internet by using Mobile IP.

A. Background on the Mobile IP Protocol

The Mobile IP protocol [7] was developed to enable the roaming in Internet of mobile nodes between different networks. Normal IP routing adopts a hierarchical addressing scheme, in which the IP address is location dependent and composed of two parts: the *network identifier* and the *host identifier*. If a mobile node moves from its home network, i.e., the network to which its IP address belong, to another network without changing address, the routers will not be able to correctly route packets addressed to it. To manage the IP mobility, the Mobile IP solution introduces two entities: the *home agent* (HA) and the *foreign agent* (FA). The HA is a host or router in the node's home network that is responsible to keep tracking the mobile node location and to tunnel packets to the node while it is away from its home network. The FA is a host or router in the mobile node's visited (foreign) network, which registers the entrance of mobile nodes, detunnels and forward traffic to the visiting node. To make mobility transparent to applications and higher layer protocols, the mobile node should continue to use its home address to

receive data, even when it leaves its home network. However, when the mobile node is attached to a network other than its home network, specific procedures are executed to assign to the new node an IP address belonging to the visited network, called *care-of-address*. If the care of address is one of the addresses announced by the FA, it is known as *foreign agent care-of-address*. If the mobile node is able to acquire an IP address valid on the foreign network that it is visiting (e.g., using a DHCP server), such a care-of-address is called *co-located care-of-address*. To be able to receive packets while visiting a foreign network, the mobile nodes should register with the HA its care-of-address, which provides the information about the current mobile node's point of attachment to the Internet. To accomplish this task, the mobile node send a REGISTRATION REQUEST message directly (if it is using the co-located care-of address) or via the FA (if it using the FA care-of-address) to its HA, which in turn responds with a REGISTRATION REPLY message. Data packets sent to the mobile node's home address are intercepted by its HA, which tunnels those packets to the mobile node's care-of-address.

One of the key mechanisms in Mobile IP is the procedure for updating the location information of mobile nodes. Mobile IP uses a proactive approach since both HAs and FAs periodically broadcast AGENT ADVERTISEMENT messages to announce their presence. A mobile node uses these messages to determine whether it is attached to its home network or it is visiting a foreign network. In addition, the AGENT ADVERTISEMENT messages enable the visiting mobile nodes to discover the care-of-address of the advertised FA. When a mobile node receives AGENT ADVERTISEMENT messages from more than one FA, there are several algorithms to manage the FA selection and the handoff to a new FA, such as the Lazy Cell Switching (LCS) and the Eager Cell Switching (ECS) [19]. In addition, mobile nodes can proactively search for FAs by sending AGENT SOLICITATION messages. Upon receiving this type of message, the FA should reply with a unicast AGENT ADVERTISEMENT message to the mobile node that issued the solicitation.

B. Mobile IP-based Solutions

The key idea behind the integration of Mobile IP and ad hoc networking is to set up a Mobile IP Foreign Agent (MIP-FA) in the gateways that interconnect the ad hoc network with external networks, and to run an extended version of classical Mobile IP in the MANET. More specifically, the mobile node uses a standard ad hoc routing protocol to establish a multi-hop route with the FA to which it is registered. Then, the FA provides Internet connectivity for the ad hoc node using the Mobile IP protocol. Although the basic design principles are simple, several issues arise when adapting the Mobile IP such as to operate in multi-hop ad hoc networks. The first obstacle comes from the fact that standard Mobile IP protocol assumes that FAs and visiting nodes have link-layer connectivity, such as to rely on link-local broadcast for signalling and control. On the contrary, in multi-hop networks the broadcast is much more costly in terms of bandwidth and energy since a broadcast in an ad hoc network floods the whole network [20]. In addition, the Mobile IP protocol adopts a proactive approach for agent discovery and to handle movement detection and handoff, by broadcasting agent advertisements periodically. In some situations, this behaviour clashes with the ad hoc routing protocol operations, especially when they are executed in an on-demand manner. Finally, since the addressing architecture in ad hoc networks is usually flat, specific techniques have to be designed to allow mobile

nodes to decide whether a destination is located within the ad hoc network or in the Internet. In the remaining of this section, we review the different solutions that have been proposed to cope with these problems, both for proactive and reactive ad hoc networks, pointing out advantages and limitations of each of them.

One of the initial approaches for connecting ad hoc networks to the Internet was presented in [4]. In that paper the authors proposed an addressing scheme for ad hoc networks in which each ad hoc node participating in a single ad hoc network selects its home address from the same IP subnet. This address is then used also when participating to the ad hoc routing protocol. In particular, DSR [14] is used for routing within the ad hoc network, while normal IP source routing applies to the wired network. When a mobile node decides to participate to the ad hoc network, it will transmit a Mobile IP AGENT SOLICITATION piggybacked on a ROUTE REQUEST targeting the IP limited broadcast address (255.255.255.255). When the FA receives this message, it unicasts an AGENT ADVERTISEMENT in reply, allowing the mobile node to register with the FA. Once the registration is completed, the mobile node's HA will use Mobile IP to tunnel packets destined for the mobile node to the FA, and the FA will deliver the packets locally to the mobile node using DSR. When the mobile node wants to communicate with a node D outside of the ad hoc network, it will issue a ROUTE REQUEST targeting the node D's IP address. If the gateway believes that the node D is reachable outside the ad hoc network, it creates a special ROUTE REPLY announcing itself as the last hop in the route to D [4]. When the mobile node receives this reply, it enters the related route into its route table and utilizes it for the transmissions of data packets to the destination node.

An alternative solution to provide Internet connectivity for on-demand ad hoc networks is described in [21], and it is known as MIPMANET. In MIPMANET, mobile nodes in an ad hoc network that want Internet access register with one of the available FAs and use their home address for every communication. When registered mobile nodes want to communicate to a host on the Internet, they tunnel each packet to the foreign agent with whom they are registered, which decapsulates the packets and forwards them to the destination. The AODV routing protocol [15] is used to deliver packets between the mobile nodes and the FAs. Note that tunnelling in the ad hoc network was not needed in [4], but the MIPMANET scheme introduces this tunnelling between mobile nodes and their FAs to separate the ad hoc network from Mobile IP, and to incorporate into the on-demand routing protocol the concept of default routes. Furthermore, the mobile node cannot decide whether a destination is located within the ad hoc network or not by simply looking at the destination IP address because, in contrast to [4], no specific addressing structure is assumed in the ad hoc network. Therefore, the mobile node must initiate a route discovery process using the AODV routing protocol, targeting the designated destination. If the destination is not found within the ad hoc network, than the mobile node infers that the destination is in the wired Internet and tunnels the packets addressed to that destination to the FA. Furthermore, MIPMANET uses reverse tunnelling as defined in [22], such that an IP tunnel is established both in the forward direction (from home agent address to foreign agent care-of address) and in the reverse direction. Figure 1 illustrates the most important components of the MIPMANET scheme described so far. Concerning the agent discovery mechanisms, MIPMANET attempts to adapt Mobile IP such as to operate in a more on-demand fashion by increasing the period AGENT ADVERTISEMENT messages are flooded in the network,

and allowing FAs to periodically unicast them to registered node only. In addition, MIPMANET utilizes a new algorithm, called MIPMANET Cell Switching (MMCS), to determine when mobile nodes should register with a new foreign agent upon moving. According to this algorithm, a registered node should register with another foreign agent if it is at least two hops closer to this new foreign agent than to its previous foreign agent, for at least two consecutive agent advertisements.

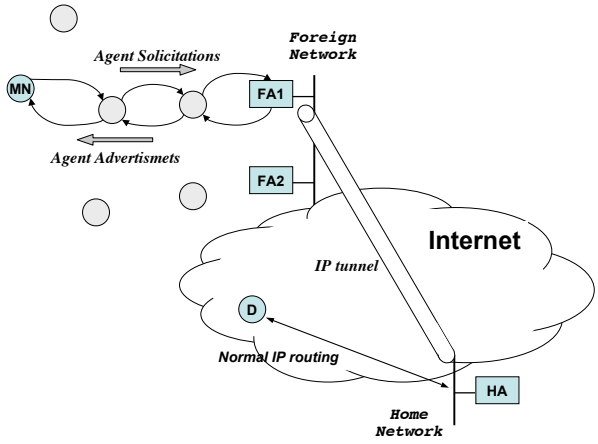

Fig. 1. Illustration of the MIPMANET solution.

In [5] a solution similar to MIPMANET is presented to implement a Mobile IP foreign agent on a gateway for ad hoc networks running the AODV routing protocol. However, the scheme proposed in [5] adopts a somehow simpler approach, limiting the use of IP tunnels inside the ad hoc network. More precisely, MIP-FA based gateways periodically advertise their presence through AGENT ADVERTISEMENT messages, such as that each mobile node can maintain a list containing the IP addresses of available FAs. A mobile node that wants Internet access can register with the closest FA one of the care-of-addresses announced in the received AGENT ADVERTISEMENT messages, and then it should update the location information maintained by its HA. In addition, mobile nodes can proactively search for foreign agents by issuing RREQ packets with destination IP address set to 224.0.0.11, which is the *All Mobility Agents* multicast group address [7]. Note that in [5] it is also proposed a duplicate-address detection scheme to enable mobile nodes to obtain a unique co-located care-of-address when no foreign agents are present in the ad hoc network. When a mobile node needs a route to a destination it initiates a normal AODV route discovery process by broadcasting RREQ messages, because the node does not know whether the destination is within the ad hoc network or in the Internet. However, when a FA receives a RREQ for a destination to which it has not an explicit route (note that the FA has explicit routes only for mobile nodes registered with it) it replies with a special RREP, called FA-RREP, with the Foreign Agent flag set, such as to indicate that the destination can be reached through the gateway. In other words, the gateway generates *Proxy* RREP packets on behalf of nodes that might be present on the Internet. Upon receiving a FA-RREP the source node does not use immediately this route, but waits

for receiving normal RREP messages indicating that the destination node is located within the ad hoc network. Moreover, by properly setting the destination sequence numbers in the RREP message it is also possible to ensure that routes to nodes in the MANET will always have higher priority than routes established using FA-RREPs sent by gateways. The advantage of using FA-RREPs is that data packets can be transmitted to the FA using standard IP forwarding and it is not needed to use tunnelling within the ad hoc network.

The solutions described so far integrate reactive ad hoc routing protocols (DSR or AODV) with the Internet routing and the Mobile IP architecture. However, the basic design of many of the Mobile IP mechanisms, such as agent discovery, movement detection and reachability of the mobile node, follows proactive principles. Thus, it is opportune to find a trade-off between the on-demand operations of reactive ad hoc routing protocols and the overhead introduced by periodically broadcasting agent advertisements. For instance, MIPMANET proposed to use the MMCS algorithm [21] to detect and move to new foreign agents. In [23] it is described a protocol that limits the flooding of agent advertisements in an n-hop neighborhood by using TTL scoping. In [24], Mobile IP is extended to manage multiple simultaneous connections with foreign networks. Based on the registered care-of addresses, multiple paths can he used for packets to and from a MH. Thus, enhanced throughput and a more reliable connection can be achieved. An alternative scheme is proposed in [25]. In that work, some heuristics are described to classify the traffic load of the gateways, such as to avoid selecting congested route to gateways. In addition, to reduce the flooding overhead due to solicitations, optimized searching algorithms are used such as the Expanding Ring Search Method [15]. However, some intrinsic limitations of on-demand routing protocols such as the inability to support default routes and to easily determine that an address is not present on the MANET, cannot be overcome without relying on complex address allocation schemes or cost-intensive IP mechanisms, such as IP-in-IP encapsulation [26]. For these reasons, recently a new architecture has been proposed to integrate Mobile IP with proactive routing protocols following a hierarchical approach [6]. More precisely, Mobile IP is used to support macro-mobility between different IP domains, while the OLSR ad hoc routing protocol is adopted to support micro-mobility inside the MANET environment. As in prior work, the architecture proposed in [6] contains a gateway implementing a MIP-FA, allowing the OLSR-IP access network to be connected to the Internet. In addition, in this hierarchical architecture special nodes, called OLSR *Base Stations*, have been introduced to reduce the number of global location updates performed by Mobile IP. These base stations have both wired and wireless interfaces and implement the OLSR protocol on both of them. When a mobile node enters an IP-OLSR access network, it will receive either periodic AGENT ADVERTISEMENT messages broadcasted by the gateways or unicast AGENT ADVERTISEMENT messages sent by the gateways in reply to the node's AGENT SOLICITATION. Note that the use of multipoint relays minimizes the overhead associated to the flooding of Mobile IP control traffic. Once the mobile node is registered, it is attached to the OLSR-IP access network. Thus, the node has a host specific entry in the routing table for each IP destination address known locally on the MANET, while all the traffic for external networks is forwarded along a possible default route out of the MANET through the gateway. The HNA messages issued by the gateway establish this binding between the gateway itself and the external networks. In such a way, it

is not needed to have an explicit procedure to determine if a destination is present or not in the MANET. Note also that the use of IP tunnelling is limited to the communications between FA and HA, but it does not occur within the ad hoc network.

Albeit the considerable effort devoted to the design of solutions enabling an efficient integration of Mobile IP with the ad hoc routing protocols to provide a global mobility between Internet and MANETs, Mobile IP-based solutions have still a number of drawbacks. The first one is that in order to allow Mobile IP and ad hoc networking to cooperate it is needed to introduce further complexities and sub-optimal operations in the implementations of both Mobile IP and ad hoc routing protocols. Probably an integrated design of Mobile IP and ad hoc routing functionalities might be much more efficient, minimizing the overheads. In addition, Mobile IP was designed to handle mobility of devices in case of relatively infrequent mobility. Thus the overheads introduced to manage roaming and handoffs between foreign agents are a relevant issue in MANET environments, where handoff functions operating at the data link layer may be more suitable. Finally, when the technique of default routes is used to route the traffic from the mobile node to the closest gateway, the use of Mobile IP can easily lead to triangle routing. In fact, when the mobile node moves it can get closer to a gateway different from the one to which it is currently registered. As a consequence, the forward traffic leaves the ad hoc network through one gateway while the return traffic enters the ad hoc network through the MIP-FA gateway to which the mobile node is registered. To solve this problem, it has been proposed the use of Mobile IP reverse tunnelling [21], or explicit tunnelling to one of the gateway instead of using default routes [27]. Note that changing between two MIP-FA based gateways do not cause a session breakage because the mobile node has simply to register the new FA with its HA. As we will discuss in the following section, changing gateways in NAT-based solutions is much more critical.

IV. Internet Connectivity using NAT-based Gateways

An alternative solution to interconnect MANETs to the Internet is to implement a Network Address Translation (NAT) modeule [8] on the gateways. Traditionally, basic NAT is used to allow hosts in a private network to transparently access the external Internet. More precisely, a router with a NAT module implemented on it, behaves as an address translator dynamically mapping the set of private addresses used internally in the local domain to a set of globally valid network addresses. A variant of basic NAT is the Network Address Port Translation, or NAPT [8], which translates private IP addresses to a single globally routable IP address by using different transport layer ports. When implementing a NAT module in a gateway of the hoc network, this gateway translates the source IP address of outgoing packets with the its IP address, which is routable on the external network. The return traffic is managed similarly, with the destination IP address (i.e., the NAT-gateway address) replaced with the IP address of the ad hoc source node.

One of the earliest implementation of this method for reactive ad hoc networks was developed by the Uppsala University for the AODV routing protocol [28]. In that implementation mobile nodes are not aware of the available gateways enhanced with NAT capabilities, and these gateways use Proxy RREP messages to reply to RREPs destined for host on the Internet. The use of Proxy RREP messages is clearly inspired by work done in [4], [5]. To reduce

the complexity of the implementation, the AODV-UU NAT solution assumes that all the addresses on the ad hoc network are allocated from the same private IP subnet. Thus, the gateways will reply only to RREQ messages targeting destinations external to the ad hoc network. To avoid this limitation, it is possible to apply solutions similar to the ones defined in [5] for a MIP-FA based gateway. More precisely, the NAT-based gateway can be allowed to reply to all the received RREQ messages generating a Proxy RREP with the same sequence number of the received RREQ. In this way, a direct route to the designated destination not traversing the gateway will always have preference on the route announced by Proxy RREP messages.

Solutions based on the use of Proxy RREPs do not work correctly in multi-homed networks, i.e., when multiple gateways are present in the ad hoc network. Indeed, to avoid session breakages it is necessary to ensure that each packet from the same session is routed over a specific gateway since a NAT router translates both outgoing and incoming packets. However, it is difficult to control the gateway selection for an ad hoc node that is moving. To solve this problem, in [29] it is described an alternative approach to provide Internet connectivity for on-demand routing protocols. First of all, the solution proposed in [29] defines a method for implementing gateway discovery using the AODV protocol. When a mobile node searches a route to its designated destination, it initially floods the network with normal RREQ messages. If the source node does not receive any reply, it issues a special RREQ message with a "Gateway"-flag set. Upon receiving this type of RREQ messages the gateways are allowed to reply with Proxy RREPs on behalf of external nodes. When the source node receives these replies, it becomes aware of the available gateways. Then, the ad hoc node selects one of these gateways according to some heuristic and it tunnels the packets addressed to external destinations to the selected gateway using for example IP-in-IP encapsulation [26]. Furthermore, the NAT will also tunnel the incoming packets returning from the Internet to the source nodes. Figure 2 illustrates how the IP-in-IP encapsulation method works when tunnelling the packets for an external host via a NAT-based gateway.

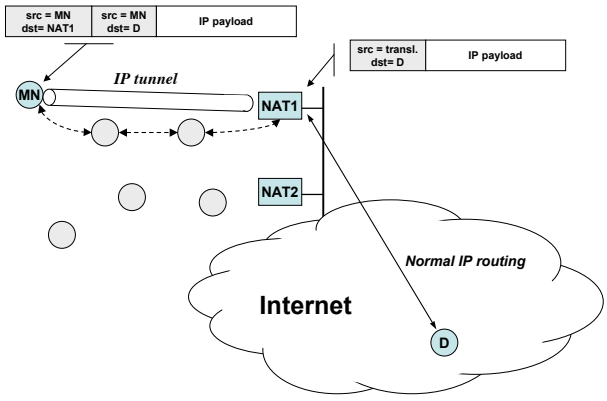

Fig. 2. Illustration of the tunnelling operations in NAT-based solutions [27], [29].

As described in [27], NAT-based gateways can be implemented also in proactive ad hoc networks. However, instead of using default routes to send packets addressed to host located in the external Internet as proposed in [6], the source node should tunnel the packets, e.g., by using IP-in-IP encapsulation [26] or minimal IP encapsulation [30], to the IP address of the closest gateway. Using explicit tunnelling instead of default routes ensures that each packet of the same transport layer session is consistently routed through the same gateway, even if the source node moves. In papers [29] and [27] it is also addressed the problem of how enabling gateways adopting different mechanisms to cooperate while providing Internet connectivity. For instance, in multi-homing scenario some gateways may be NAT-based, and other gateways may be MIP-FA based. Again, a working solution for this issue is the use of explicit tunnelling that forces the packets generated from the same session to be routed the gateway selected at the beginning of the session itself. This prevents the session break when the source node gets closer to another gateway. However, this method requires that special techniques are implemented such as to allow source nodes to discover the different capabilities of the available gateways. To this end, extensions of the ad hoc routing protocols have to be devised. Finally, it is worth pointing out that most of the schemes described in this section rely heavily on the use of IP tunnels. However, tunnelling introduces a fixed overhead in the tunnelled IP packet headers. For instance, in case of IP-in-IP encapsulation 20 bytes of overhead are added in every outgoing packet. Experimental results presented in [27] indicate that in some situations the throughput obtained by a TCP session can suffer a 30% decrease. This clearly motivates the need of designing more efficient and lightweight solutions to provide Internet connectivity for ad hoc networks.

V. A Layer-2 Approach to Internet Connectivity for Ad Hoc Networks

The basic design principles we adopted during the definition of our proposal was to provide transparent communications between static nodes (using traditional wired technologies) and mobile nodes (using ad hoc networking technologies), employing mechanisms that run below the IP layer. As discussed in the introduction, in this work we address two major problems: node address self-configuration and global Internet connectivity. However, before describing the details of our solutions, it is useful to illustrate the complete network architecture we propose for interconnecting ad hoc networks to the Internet. To this end, Figure 3 depicts the reference network model we consider in this work.

As shown in the figure, we envision that mobile/portable nodes far away from the fixed networking infrastructure establish multi-hop wireless links to communicate with each other (e.g., using IEEE 802.11 technology [3]). Special nodes, denoted as gateways, with both wired and wireless interfaces, are used to connect the ad hoc components to a wired LAN (e.g., an Ethernet-based LAN). In our architecture, it is permitted the multi-homing, i.e., the presence of multiple gateways within the same ad hoc component. Consequently, specific mechanisms are required to support the handoff between gateways without TCP-connection breaks. In general, between pairs of gateways in radio visibility of each other, two direct links can be established, both wired and wireless. The choice between the two links is demanded to the routing protocol. However, we can assume that the wired link has a lower link cost than the wireless link because wired technologies are still more reliable and have higher capacity than standard

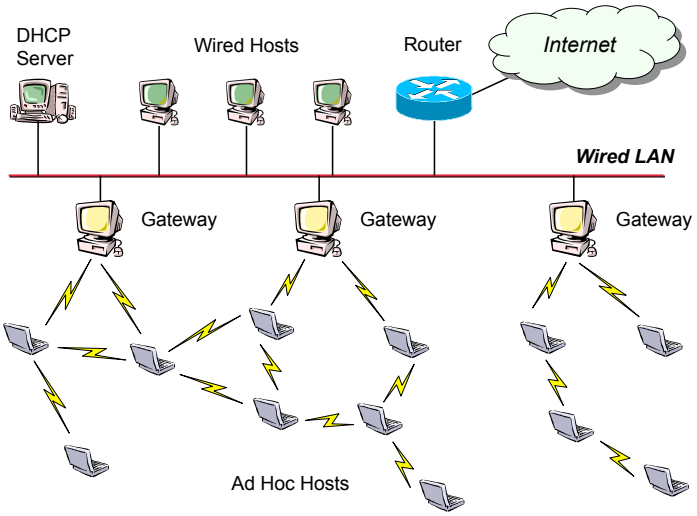

Fig. 3. Reference Network Model.

wireless technologies. As a consequence, a routing protocol selecting least-cost paths will always give preference to the wired path for inter-gateway communications. In Section V-B, we will explain in depth the implications of this assumption. The other key feature that we assume to be valid in the network concerns the addressing structure. More precisely, we make the assumption that all the nodes in the extended LAN, both ad hoc nodes and static ones, have an IP address with the same network identifier. This implies that hosts in the external Internet consider the extended LAN as a single IP subnet. To indicate the network identifier we use the standard notation IP_S/L, in which IP_S indicates the network prefix, and L is the network mask length.

Standard IP routing is used to connect the extended LAN to the Internet. However, a specific ad hoc routing protocol is needed to enable multi-hop communications among the ad hoc nodes. The scheme described in the following has been designed for being integrated with proactive routing protocols (such as the Optimized Link State Routing (OLSR) protocol [16] or the Topology Dissemination Based on Reverse-Path Forwarding (TBRF) routing protocol [17]). The motivation behind this design choice is that proactive routing protocols usually support gateway advertisements, allowing these nodes to use special routing messages to set up default routes in the ad hoc network. As explained in Section III, default routes are an efficient mechanism to forward traffic that does not have an IP destination locally known to the ad hoc network. In addition, proactive routing protocols, adopting classical link state approaches, build a complete network-topology knowledge in each ad hoc node. This topology information could significantly simplify the operations needed to acquire Internet connectivity. In this work, the reference ad hoc routing algorithm is OLSR, but our architecture is general and it is equally applicable to other proactive routing protocols.

The following sections describe the operations performed by our proposed techniques and how the ad hoc

components are transparently integrated in the wired infrastructure.

A. Ad Hoc Node Self-Configuration

In traditional networks, hosts rely on centralized servers like DHCP [31] for obtaining IP configuration parameters (i.e., a unique IP-based address, a common netmask and, eventually, a default gateway), but this cannot be easily extended to MANETs because of their distributed and dynamic nature. Thus, various protocols have been proposed recently in the literature for the purpose of address self-configuration in MANETs. In general, with protocols using stateless approaches nodes arbitrarily select their own address, and a Duplicate Address Detection (DAD) procedure is executed to verify its uniqueness and resolve conflicts. On the other hand, protocols based on stateful approaches execute distributed algorithms to establish a consensus among all the nodes in the network on the new IP address, before assigning it. The protocols proposed in [32] and [33] are examples of the latter and former approach, respectively, while [34] presents a general overview of the several solutions currently available. Generally, all these protocols assume reliable flooding in order to synchronize nodes' operations and resolve inconsistencies in the MANET, but this is difficult to be guaranteed in ad hoc networks. Another main limitation of these solutions is that they are designed to work in *stand-alone* MANET, while no protocols have been devised to take fully advantage of the access to external networks. In addition, the problems of selecting a unique node address, routing the packets and accessing the Internet are still separately addressed, while a unified strategy may be beneficial, reducing complexities and overheads.

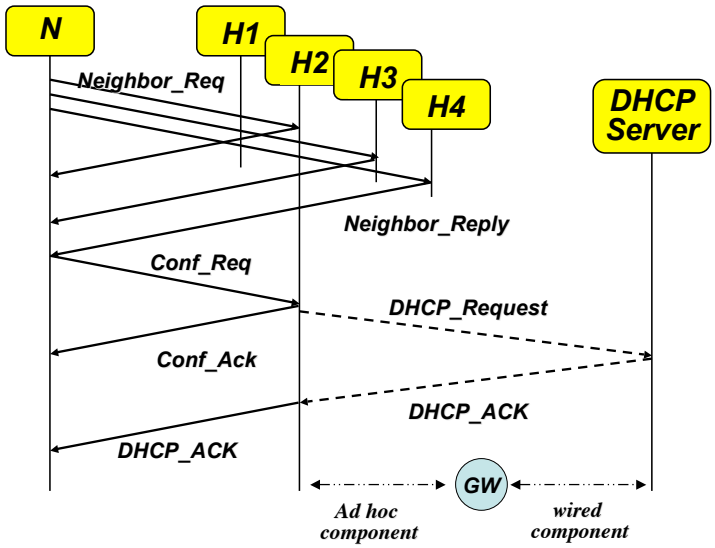

Fig. 4. Message exchanges during the ad hoc node self-configuration.

The method we propose to assign a unique IP address to each ad hoc node treads the footprints of the technique described in [33]. In that paper, a preliminary message handshake was used to discover a reachable MANET node that could act as initiator of the configuration process. Similarly, in our proposal there is an initial message

handshake to elect one of the neighboring ad hoc nodes as DHCP relay agent for the new node joining the ad hoc component. As illustrated in Figure 4, node *N* broadcasts special messages, called NEIGHBOR_REQ, to discover other nodes that are within its radio visibility and that can interconnect him to the ad hoc component. To make more robust the protocol to messages losses and various network configurations, node *N* can periodically generate new NEIGHBOR_REQ messages scanning each channel and operating mode (e.g., 802.11*abg*) supported by its interface. When a node that is already part of the ad hoc network correctly receives a NEIGHBOR_REQ message, it discovers the physical address of the node *N* and it can unicast a NEIGHBOR_REPLY message to node *N*. From the received NEIGHBOR_REPLY messages, node *N* can build a list of available proxy DHCP relay agents, and it will select one of them according to some heuristic (e.g., the one with the best signal quality, or the last one to reply). In the example shown in Figure 4, node *N* has selected node *H*2 as its proxy agent. Node *H*2 is informed about this choice through a CONF_REQ message. As soon as node *H*2 receive this request it activates its DHCP relays agent and initiates the process of address assignment on behalf of node *N* using the standard DHCP protocol. Note that node *H*2 can contact the DHCP servers located in the wired LAN using unicast DHCP control messages, because node *H*2 is part of the ad hoc component and, therefore, it has all the IP parameters needed to communicate. The DCHP messages generated by node *H*2 are routed through one of the gateways according to the mechanisms that will be described in the following section. The DHCP server receiving the request, will answer to the DHCP relay agent with a DHCP_ACK, containing the IP configuration parameters. The configuration process is concluded when the DHCP Relay forwards the DHCP_ACK message to the initial node *N* that is now configured and can join the network. After joining the network, node *N* may also turn itself into a DHCP relay agent for the DHCP server from which it received the IP configuration parameters, letting other nodes to subsequently joining the ad hoc component. Finally, it is worth noting that it is not needed any initialization procedure for the ad hoc network, because the gateways are directly connected to the wired LAN and can broadcast a DHCP_DISCOVER message to locate available servers. In this way, the first mobile node to enter the ad hoc network may find at least one gateway capable of initiating the illustrated configuration process.

B. Interconnecting the ad hoc nodes with the Internet

The basic assumptions of our proposal are: *i*) that the ad hoc part of the extended LAN implements a proactive routing protocol such as that each node has a routing table with entries that specify the IP address of the next-hop neighbor to contact to send a packet destined to any other host or subnetwork; and *ii*) all the hosts in the extended LAN shares the same IP prefix. The methods we propose to interconnect the ad hoc components of the extended LAN illustrated in Figure 3 rely on the use of default routes and some extended functionalities of the ARP protocol. For clarity, in the following we separately describe how communications are established and maintained between ad hoc nodes and hosts in the wired LAN (i.e., Intranet communications) or hosts in the external Internet (i.e., communications routed through the default router *R* shown in Figure 3). However, before describing the proposed mechanisms it is useful to give a short description of the ARP protocol, whose functionalities will be extensively exploited in our proposal.

C. ARP Protocol

IP-based applications address a destination host using its IP address. On the other hand, on a physical network individual hosts are known only by their physical address, i.e., MAC address. The ARP protocol [35] is then used to translate, inside a physical network, an IP address into the related MAC address. More precisely, the ARP protocol broadcasts the ARP_REQUEST message to all the hosts attached to the same physical network. This packet contains the IP address the sender is interested in communicating with. The target host, recognizing that the IP address in the packet matches its own, returns its MAC address to the requester using an unicast ARP_REPLY message. To avoid continuous requests, the hosts keep a cache of ARP responses.

In addition to these basic functionalities, the ARP protocol has been enhanced with more advanced features. For instance in [36] it has been proposed the *Proxy-ARP* mechanism, which makes it possible to construct local subnets. Basically, the Proxy ARP technique allows one host to answer the ARP requests intended for another host. This mechanism is particularly useful when a router connects two different physical networks, say *NetA* and *NetB*, belonging to the same IP subnet. By enabling the Proxy ARP on the router's interface attached to *NetB*, any host A in *NetA* sending an ARP request for a host B in *NetB*, will receive as response the router's MAC address. In this way, when host A sends IP packets for host B, they arrive to the router, which will forward such packets to host B.

1) Intranet connectivity.: First of all, let us consider an ad hoc node *N* that want to communicate with a wired host *H* located in the wired LAN to which the ad hoc network is interconnected. Since the ad hoc nodes implement a proactive routing protocol, their routing tables contain host-specific entries to reach any other node in the ad hoc network. In addition the routing table is populated with the default routes flooded in the network by the gateways. As discussed in Section II-B gateways advertise Internet connectivity through the $0.0.0.0/0$ default route. Another entry that is automatically inserted by the TCP/IP protocol stack at the network boot is the one related to the local reachability. More precisely, if the node *N*'s IP address belongs to the IP subnet identified by the $\mathrm{IP_S}/\mathrm{L}$ network/mask pair, then in the node *N*'s routing table there is an entry that assumes all the address matching this network prefix as attached to the same physical segment. As a consequence, when the node *N* wants to send a packet addressed to node *H*, it believes node *H* as directly reachable and issues an ARP_REQUEST message targeting node *H*'s physical address. However, this request will fail because the ARP protocol cannot correctly operate with multi-hop communications. To solve this inconsistency, node *N* needs a specific mechanism to discover that node *H* is not located on the same physical segment, although it shares with node *N* the same network prefix. To this end, we exploit the properties of both default routes and longest-matching rules used by the standard IP routing. More precisely, we configure the gateways such as to advertise two additional default routes, which announce the reachability of the wired LAN. These default routes are $\mathrm{IP_{SL}}/(\mathrm{L}+1)$ and $\mathrm{IP_{SU}}/(\mathrm{L}+1)$, i.e., two IP subnets such as that the union of these two sets is equal to $\mathrm{IP_S}/\mathrm{L}$. In this way, each mobile host will have, for any host on the local wired LAN, a routing table entry with a more specific network/mask than the one related to its wireless interface. Note that the use of these additional default routes may cause problems for the gateways. In fact, being part of

the ad hoc component, the gateways will receive HNA messages sent by other gateways, setting up the additional routing entries advertised in these messages. However, when a gateway wants to send packets to a wired host on the local wired LAN (e.g., node H), the routing table lookup will choose one of these two entries, instead of the entry related to its wired interface . The effect is that the IP packet will loop among the GW nodes until the TTL expires, without reaching the correct destination H. To resolve this problem, we statically add in each gateway two routing entries related to its wired interface. These two additional entries have the same network/mask as the two announced in the HNA messages (i.e., $\mathrm{IP_{SL}}/(\mathrm{L}+1)$ and $\mathrm{IP_{SU}}/(\mathrm{L}+1)$), but with lower metric. In this way, when a gateway want communicate with an host in the wired LAN, it will give preference to its wired interface rather than the wireless interface.

Let us consider the reverse direction, i.e., a wired host H that want to communicate with an ad hoc node N. Again, node H believes node N on its same physical segment and it will issue an ARP_REQUEST message targeting node N's physical address, which cannot be received by node N. To solve this problem, we activate a Proxy ARP server on the wired interfaces of each gateway. When a gateway will receive a ARP_REQUEST searching for an IP address that is reachable through the gateway's wireless interface, then it publish its MAC address such as to receive the local traffic targeting that IP address. When the gateway receives a pachek for an IP address that it is publishing through the Proxy ARP, it will use the ad hoc routing protocol to forward the packet to the designated destination inside the ad hoc network. Note that, each gateway publish only the IP address that have an entry in its routing table with netmask 255.255.255.255, and next hop on the gateway's wireless interface to be sure that it is the closest gateway to the ad hoc node having that IP address.

There are some network configurations where asymmetric routing may occur, i.e., the forward path is different from the return path. For instance, let us consider the case in which node N is in radio visibility of two gateways, say $GW1$ and $GW2$. In this situation, the OLSR routing algorithm will randomly select one of these gateways as default gateway for node N. However, both gateways are allowed to send ARP replies for ARP requests issued by node H for the node N's IP address. In this case, the wired node H will update its ARP table using the information delivered in the last received ARP REPLY. Let us assume that $GW1$ is the default gateway for node N, but $GW2$ has sent the last ARP reply to node H. In this case, node H sends the traffic destined to node N to $GW2$, which routes it to node N. On the other hand, node N sends packets destined to node H to $GW1$, which forwards them to node H. It is important to note that asymmetric paths are not by themselves a problem. Indeed, both node N and node H correctly receive and send their packets. In addition the asymmetric routing occurs only in symmetric topologies. Thus, it is reasonable to assume, in this local environment, that both paths are characterized by similar delays.

2) Internet connectivity.: Providing Internet connectivity for the ad hoc nodes is now intuitive since Internet connectivity can be considered as a special case of the Intranet connectivity explained above. The only additional requirements is that the gateway knows the default router's IP address. However, the default router for the LAN is one of the IP configuration parameters that is provided in the DHCP_ACK messages used to configure both

wired hosts and ad hoc nodes. Thus, when a node want to send a packet to an IP address to which has not specific information in its routing table, it will simply forward the packet to the gateway. Then, the gateway will deliver the packet to the default router using the same mechanisms adopted to communicate with any wired host in the LAN. Similarly the incoming traffic received from the Internet and targeting the IP address of an ad hoc node, will be forwarded by the default router to the gateway that operates the Proxy ARP for that IP address.

3) Mobility support.: In general, solutions to support Internet connectivity for ad hoc networks, which are based on gateways, experience TCP-session breaks when the default route changes, depending on dynamics and mobility in the network. To avoid that TCP sessions break, in [29] it was proposed to replace default routes with explicit tunneling between the mobile nodes and the gateways. However, this complicates significantly the implementation and introduces relevant overheads. On the contrary, in our architecture the mobility is supported in a transparent way for the higher protocol layers. Indeed, the only effect of changing the default gateway for an ad hoc node, is that its outgoing traffic is routed towards the new gateway (e.g., $GW2$), while the initial gateway (e.g., $GW1$) continues to receive the incoming traffic and to forward it to designated ad hoc node. This results into asymmetric routing. However, this condition has not effect on the state of the transport layer connection. In addition, this asymmetry can be easily removed by using an advanced feature of the ARP protocol. More precisely, when $GW2$ becomes aware that the next hop for the designated ad hoc node, say N, switches from its wired interface to its wireless interface, it generates a *Gratuitous ARP* on the wired interface for node N's IP address. This will update the ARP table in all the wired hosts that have an old entry for the node N's IP address, which was mapped with the MAC address of GW1's wired interface. This action restores a symmetric path for the active packet flows destined to and/or originated from node N.

VI. Implementation and Measurements

We have prototyped the core functionalities of our architecture. In particular, we have developed the software components described in Section V-B, concerning the support of Internet and Intranet connectivity for the ad hoc nodes. In our test-beds we have used a number of *IBM R-50* laptops with *Intel Pro-Wireless 2200* as integrated wireless card. The IP addresses for these laptops have been statically assigned. We have used the OLSR_UniK implementation for Linux in version 0.4.8 [37] as ad hoc routing protocol. The installed Linux kernel distribution was 2.6.9. The ad hoc nodes are connected via IEEE 802.11*b* wireless links, transmitting at the maximum rate of 11 Mbps. To generate the asymptotic UDP and TCP traffic during the experiments we used the *iperf* tool[1]. If not otherwise specified, the packet size is constant in all the experiments and the transport layer payload is equal to 1448 bytes. Differently from other studies such as [27], in which the network topology was only emulated by using the *IP-tables* feature of Linux, our experiments were conducted in realistic scenarios, with hosts located at the ground floor of the CNR building. The experimental results reported in the following section are based on measurements taken from the testbed illustrated in Figure 5

[1] `http://dast.nlanr.net/Projects/Iperf/`.

Fig. 5. Internet access testbed.

A. Experimental Results

We compute the impact of the number of hops needed to reach the gateway on the throughput performance of a single TCP and UDP flows. In the test, an *iperf* server (termination of the traffic sessions) runs on a static host in the wired LAN, while the *iperf* clients (originators of traffic sessions) have been set up on the mobile nodes. Concerning the parameters specific to the OLSR protocol, in Table I we summarize the setting used during the experiments. Note that this setting is not the default configuration for the OLSR specific parameters as specified

TABLE I
SETTING OF OLSR SPECIFIC PARAMETERS.

Parameter	Value
HELLO_INTERVAL(s)	0.5s
NEIGHB_HOLD_TIME(s)	6s
TC_INTERVAL(s)	1.25s
TOP_HOLD_TIME(s)	15 s
HNA_INTERVAL(s)	1.25s
HNA_HOLD_TIME(s)	15 s
Hysteresis	no

in [16]. However, this setting is the one that provided the best tradeoff between throughput and routing overheads. The reader is referred to [38] to find a more detailed discussion on these aspects and a larger series of measurement results.

Figure 6 shows the UDP and TCP throughput obtained during a single experiment, as a function of the time and for different chain lengths. Several observations can be derived from these experimental results. First, we can note that the maximum UDP throughput is always greater than the maximum TCP throughput. This is obviously due to

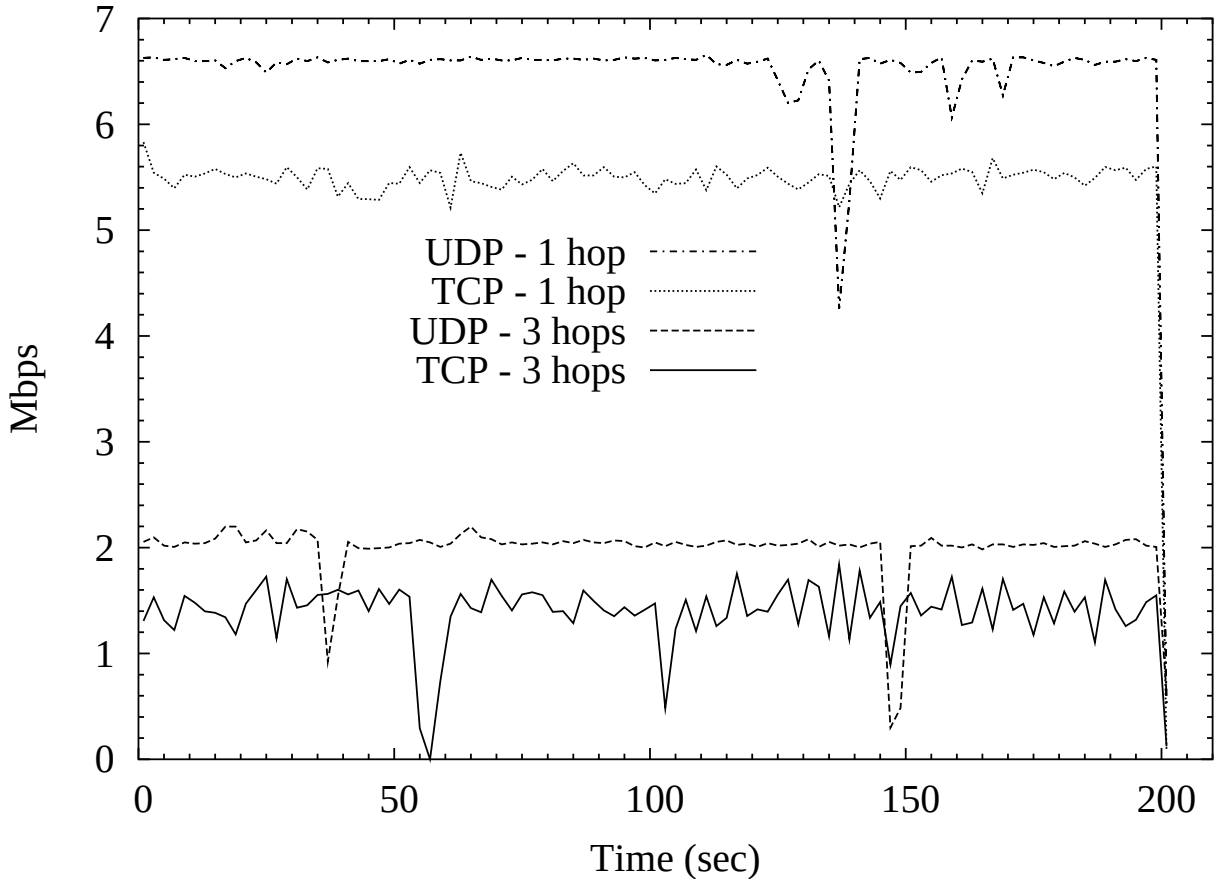

Fig. 6. Comparison of UDP and TCP throughputs for different chain lengths.

the additional overheads introduced by the TCP return traffic, which consists of TCP ACK packets. In addition, as expected, the longer the route, the lower is the peak throughput achieved by the session flow (both TCP and UDP). The figure also shows that the throughput, although not frequently, suffers sharp decreases. Two are the main causes of these throughput degradations. One is related to the radio interferences that is introduced by external sources and channel noise (note that the experiments were conducted during working hours in the CNR building), which may reduce the channel capacity. The second one is that collisions and channel errors can cause OLSR message losses, inducing the temporary timeout of valid routes. It is worth pointing out that these phenomena are not very critical in static configurations, at least with an appropriate configuration of the OLSR specific parameters. However, when mobility is introduced the holes in TCP and UDP throughput are more frequent and last longer because OLSR may require a significant amount of time to recompute a valid route towards a new gateway.

VII. Concluding Remarks

In this chapter we have reviewed the solutions described in the literature for connecting an ad hoc network to the Internet. The unique characteristics of ad hoc networking have relevant implications when adapting techniques primarily designed for the fixed Internet, such as the Mobile IP standard. We have discussed which are the

architectural issues that arise when using Mobile IP for Internet access in a multi-hop ad hoc network, focusing on the impact of using multi-hop communications, the lack of a centralized and hierarchical addressing scheme, and the cost of network-wide broadcasts. We have also outlined another possible solution based on the use of NAT modules implemented on the gateways, but generally these schemes use explicit IP tunneling to manage mobility, introducing additional overheads. Considering these limitations, in this chapter we have also described a practical architecture to interconnect an ad hoc network to the Internet by integrating the ad hoc network in a traditional wired LANs. Differently from previous solutions, we locate our architecture below the IP level, such as to design a lightweight and efficient ad hoc support framework, which is easy to be implemented and introduces minimal overheads. An implementation based on the OLSR protocol has been realized to validate the effectiveness of this architecture.

We believe that there are several related aspects that are worth being further investigated in future work.

- The gateway selection procedure implicitly relies on the ad hoc routing protocol. In the case of OLSR, it is accomplished according to a shortest-path basis. However, in a multi-homing scenario, several gateways can exist, which may be implemented using different technologies and may have different capabilities. Thus, there could be many benefits in designing cooperative heuristics to select gateways such as to obtain load balancing within the ad hoc network, or more efficient handovers.
- In this work we have considered basic IP services, i.e., unicast routing and dynamic address allocation. However, more sophisticated functionalities, such as multicast and QoS management, have been developed for the Internet. Therefore, the proposed architecture should be extended to integrate these additional capabilities.
- The address allocation scheme described in this chapter allows the exploitation of DHCP servers to assign IP addresses that are topologically correct in the entire extended LAN. However, there is not a detailed evaluation of efficiency of this proposal or a comparative analysis with different node auto-configuration schemes. In addition, it should be explored how to extend our solution to deal with the typical problems that may arise due to mobility of nodes, such as message losses, and network partition and merger.

REFERENCES

[1] F. F. Programme, "MobileMAN – Mobile Metropolitan Ad hoc Networks," IST-2001-38113, October 2002. [Online]. Available: http://cnd.iit.cnr.it/mobileMAN/

[2] R. Bruno, M. Conti, and E. Gregori, "Mesh Networks: Commodity Multihop Ad Hoc Networks," *IEEE Communications Magazine*, vol. 43, no. 3, pp. 123–131, March 2005.

[3] *Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specification/Amendment 2: Higher-speed Physical Layer (PHY) in the* 2.4 *GHz band*, The Institute of Electrical and Electronics Engineer Std. 802.11b, Nov. 2001.

[4] J. Broch, D. Maltz, and D. Johnson, "Supporting hierarchy and heterogenous interfaces in multi-hop wireless ad hoc networks," in *Proc. of I-SPAN'99*, Perth, Australia, June, 23–25 199, pp. 370–375.

[5] Y. Sun, E. Belding-Royer, and C. Perkins, "Internet Connectivity for Ad hoc Mobile Networks," *International Journal of Wireless Information Networks*, vol. 9, no. 2, pp. 75–88, April 2002, Special issue on "Mobile Ad hoc Networks: Standards, Research, Application".

[6] M. Benzaid, P. Minet, K. Al Agha, C. Adjih, and G. Allard, "Integration of Mobile-IP and OLSR for a Universal Mobility," *Wireless Networks*, vol. 10, no. 4, pp. 377–388, July 2004.

[7] C. Perkins, "IP Mobility Support for IPv4," RFC 3344, August 2002. [Online]. Available: http://www.ietf.org/rfc/rfc3344.txt

[8] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," RFC 2663, August 1999. [Online]. Available: http://www.ietf.org/rfc/rfc2663.txt

[9] A. Acharya, A. Misra, and S. Bansal, "A Label-switching Packet Forwarding Architecture for Multi-hop Wireless LANs," in *Proc. of ACM WoWMoM 2002*, Atlanta, Georgia, USA, September, 28 2002, pp. 33–40.

[10] C. Tschuding, R. Gold, O. Rensfelt, and O. Wibling, "LUNAR: a Lightweight Underlay Network Ad-hoc Routing Protocol and Implementation," in *Proc. of NEW2AN'04*, St. Petersburg, Russia, February, 2–6 2004.

[11] R. Draves, J. Padhye, and B. Zill, "The architecture of the Link Quality Source Routing Protocol." Microsoft Research, Tech. Rep. MSR-TR-2004-57, 2004.

[12] Internet Engineering Task Force (IETF). (2006) Mobile Ad-hoc Networks (MANET) – Workgroup. [Online]. Available: http://www.ietf.org/html.charters/manet-charter.html

[13] E. Belding-Royer, *Routing Approaches in Mobile Ad Hoc Networks*. New York, NY: IEEE Press and John Wiley & Sons, 2003.

[14] D. Johnson, D. Maltz, and Y.-C. Hu, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," Internet Draft, July 19 2004. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[15] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, July 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3561.txt

[16] T. Clausen and P. Jaquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626, October 2003. [Online]. Available: http://www.ietf.org/rfc/rfc3626.txt

[17] R. Ogier, F. Templin, and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)," RFC 3684, February 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3684.txt

[18] Z. Haas, M. Pearlman, and P. Samar, "The Zone Routing Protocol (ZRP) for Ad Hoc Networks," Internet Draft, July 2002.

[19] C. Perkins, *Mobile IP Design Principles and Practice*. Prentice Hall, January 1998.

[20] S. Ni, Y. Tseng, Y. Chen, and J. Sheu, "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *Wireless Networks*, vol. 8, no. 2/3, pp. 153–167, 2002.

[21] U. Jönsson, F. Alriksson, T. Larsson, P. Johansson, and G. Maguire Jr., "MIPMANET - Mobile IP for Mobile Ad Hoc Networks," in *Proc. of MobiHoc 2000*, Boston, MA, USA, August, 11 2000, pp. 75–85.

[22] G. Montenegro, "Reverse Tunneling for Mobile IP," RFC 2344, May 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2344.txt

[23] P. Ratanchandani and R. Kravets, "A Hybrid Approach to Internet Connectivity for Mobile Ad hoc Networks," in *Proc. of IEEE WCNC 2003*, vol. 3, New Orleans, USA, March, 16–20 2003, pp. 1522–1527.

[24] C. Ahlund and A. Zaslavsky, "Integration of Ad Hoc Network and IP Network Capabilities for Mobile Hosts," in *Proc. of ICT'2003*, vol. 1, Tahiti, February 23 –March 1 2003, pp. 482–489.

[25] R. Brannstrom, C. Ahlund, and A. Zaslavsky, "Maintaining Gateway Connectivity in Multi-hop Ad hoc Networks," in *Proc. of IEEE LCN 2005*, Sydney, Australia, November 15–17 2005, pp. 682–689.

[26] C. Perkins, "IP Encapsulation within IP," RFC 2003, October 1996. [Online]. Available: http://www.ietf.org/rfc/rfc2003.txt

[27] P. Engelstad, A. Tønnesen, A. Hafslund, and G. Egeland, "Internet Connectivity for Multi-Homed Proactive Ad Hoc Networks," in *Proc. of IEEE ICC'2004*, vol. 7, Paris, France, June, 20–24 2004, pp. 4050–4056.

[28] AODV-UU Implementation. Version 0.6. Uppsala University. [Online]. Available: http://core.it.uu.se/AdHoc/AodvUUImpl

[29] P. Engelstad and G. Egeland, "NAT-based Internet Connectivity for On Demand MANETs," in *Proc. of WONS 2004*, Madonna di Campiglio, Italy, January, 18–23 2004, pp. 4050–4056.

[30] C. Perkins, “Minimal Encapsulation within IP,” RFC 2004, October 1996. [Online]. Available: http://www.ietf.org/rfc/rfc2004.txt

[31] R. Droms, “Dynamic Host Configuration Protocol,” RFC 2131, March 1997. [Online]. Available: http://www.ietf.org/rfc/rfc2131.txt

[32] N. Vaidya, “Weak Duplicate Address Detection in Mobile Ad Hoc Networks,” in *Proc. of ACM MobiHoc 2002*, Lausanne, Switzerland, June, 9–11 2002, pp. 206–216.

[33] S. Nesargi and R. Prakash, “MANETconf: Configuration of Hosts in a Mobile Ad Hoc NEtwork,” in *Proc. of INFOCOM 2002*, vol. 2, New York, NY, June, 23–27 2002, pp. 1059–1068.

[34] K. Weniger and M. Zitterbart, “Address Autoconfiguration on Mobile Ad Hoc Networks: Current Approaches and Future Directions,” *IEEE Network*, vol. 18, no. 4, pp. 6–11, July/August 2004.

[35] S. Carl-Mitchell and J. Quarterman, “Using ARP to Implement Transparent Subnet Gateways,” RFC 1027, October 1987. [Online]. Available: http://www.ietf.org/rfc/rfc1027.txt

[36] D. Plummer, “An Ethernet Address Resolution Protocol,” RFC 826, November 1982. [Online]. Available: http://www.ietf.org/rfc/rfc0826.txt

[37] A. Tønnesen. (2004, December) Implementation of the OLSR specification (OLSR_UniK). Version 0.4.8. University of Oslo. [Online]. Available: http://www.olsr.org/

[38] E. Ancillotti, R. Bruno, M. Conti, E. Gregori, and A. Pinizzotto, “A Layer-2 Architecture for Interconnecting Multi-hop Hybrid Ad Hoc Networks to the Internet,” in *Proc. of WONS 2006*, Les Menuires, France, January, 18–20 2006.