A Protocol for Macro Mobility and Multihoming Notification in Wireless Mesh Networks

Rainer Baumann, Olga Bondareva, Simon Heimlicher, Martin May
Computer Engineering and Networks Laboratory
ETH Zurich, Switzerland
{baumann,bondareva,heimlicher,may}@tik.ee.ethz.ch

***Abstract*— Wireless mesh networks are cost-efficient means to provide ubiquitous Internet access. For building large-scale wireless mesh networks, multiple access networks are joined together into one large network. In such large networks, nodes have to communicate with the Internet via multiple access gateways. The problem in such scenarios is how to make mesh nodes aware of the gateway over which data is sent towards the Internet. The goal of this paper is to propose a routing protocol-independent method that allows nodes to (i) determine when they are switching the access network; (ii) to support switching of access networks; and (iii) to support multihoming.**

I. Introduction

Internetworking between wireless mesh networks and the Internet is a cost-efficient way of offering ubiquitous Internet access. In such wireless mesh networks, the interconnection with the Internet is provided by gateways connected to access networks. In large-scale wireless mesh networks, multiple gateways are attached to a multitude of different access networks (see Fig. 1). When a node in the wireless mesh network communicates with a node in the Internet, the IP packets are relayed through the mesh to any of the available gateways. As a result, when a node moves, routes in the mesh network might change and its IP traffic is forwarded to another gateway. If these two gateways belong to the same access network, we refer to this kind of mobility as *micro mobility*, whereas if they belong to different access networks, we refer to it as *macro mobility*. There are situations, where a node is attached to multiple gateways at a time. When these gateways belong to multiple access networks we refer to the node as *multihomed* node [1].

For enabling macro mobility and multihoming, several IP mobility management protocols and extensions have been proposed [2]–[4]. They all require that a node is aware of the access networks it is attached to. However, the selection of the access network depends on the routing and forwarding strategy implemented in the wireless mesh network. There are two possible mechanisms: service discovery or anycast routing. In the first case, a node uses a gateway discovery protocol to find neighboring gateways (see [5]–[7]). Based on this information a node decides which gateway to use for relaying packets to the Internet. Then, packets are sent to the chosen gateway by means of unicast. With anycast routing, a node leaves the choice of gateway to the routing protocol. A node only indicates that a packet should be sent to any gateway without specifying it (see [8], [9]). The routing protocol then routes the packets in an anycast manner to one of the gateways. In the first case, a node knows which gateway it relays its packets to and thus is aware of its macro mobility. However in the second case, the node is not aware of the selected access network and is hence not able to adapt to changes caused by its macro mobility.

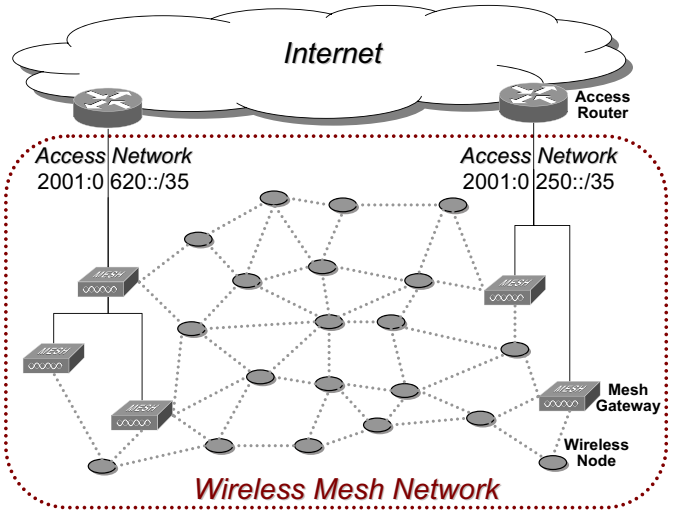

Fig. 1. A wireless mesh network connected to the Internet through different access networks.

But, since anycast is a very efficient mean to implement gateway selection in wireless mesh networks, we aim at complementing this approach by adding a notification protocol. Specifically, we propose a notification protocol that is driven by the gateways and that is independent of the used routing protocol. In our approach, the gateway detects the macro mobility of nodes by monitoring the source addresses of packets sent to the gateway. If the addresses do not match the access network of the gateway and the node is not multihomed, the gateway sends a notification message to the sending node with the configuration information for its new access network. This node then adjusts its configuration accordingly. If necessary, the node also informs its communication peers about its new address. In cases where the nodes are multihomed, the gateway periodically informs the mesh node that some of its packets

are relayed through its access network and performs a network address translation of the network prefix to fit the packet address to the routing topology. If necessary, the node also informs its communication peers about its additional locator address.

The rest of this paper is structured as follows. In the next section, we explain the functionality of IP mobility management protocols. Following, we present our solution to deal with macro mobility and multihoming. Then, in section IV we briefly discuss deployment issues and finally, we address future work and conclude.

II. IP Mobility Management Protocols

In this section, we discuss related work and introduce IP mobility management protocols and their extensions to support multihoming .

There are two IP mobility management protocols proposed by the IETF for enabling macro mobility in IPv6: MobileIPv6 [10] and the Host Identification Protocol (HIP) [11]. Both protocols maintain a fixed proxy (Home Agent / Rendezvous Server), a host that is aware of the current location and address of a node. This architecture enables permanent reachability even with mobile nodes. MobileIPv6 and HIP also offer an address change notification mechanism to preserve established transport sessions in the presence of macro mobility. For both of them, Internet drafts are proposed which describe extensions to enable multihoming [2]–[4]. Note however that these two IP mobility management protocols and their extensions for multihoming require that a node explicitly knows the access networks over which its packets are forwarded to the Internet. This knowledge allows a node to deal with its macro mobility or to maintain its multihoming. To deal with macro mobility, a moving node updates its address to topologically fit to the access network relaying its packets and notifies its fixed proxy as well as its communication peers about its address change. Also for multihoming, a node has to inform its communication peer about additional or outdated locators. For this purpose, each node has to maintain a list of access networks currently used.

III. Mobility Notification Protocol

In this section, we describe our notification protocol for IPv6 which allows to handle macro mobility and which also supports multihoming independently of the used routing protocol. The proposed protocol is independent from existing IP mobility management protocol, hence the protocol enables nodes in a mobile mesh network to use MobileIPv6, HIP or similar IP mobility management protocols and its multihoming extensions.

First, we give an overview of the proposed protocol and specify the mobility notification message. Then, we explain how gateways detect macro mobility and how multihoming is supported. Following, we specify the handling of mobility notification messages at the mobile nodes as well as the procedure for node joins.

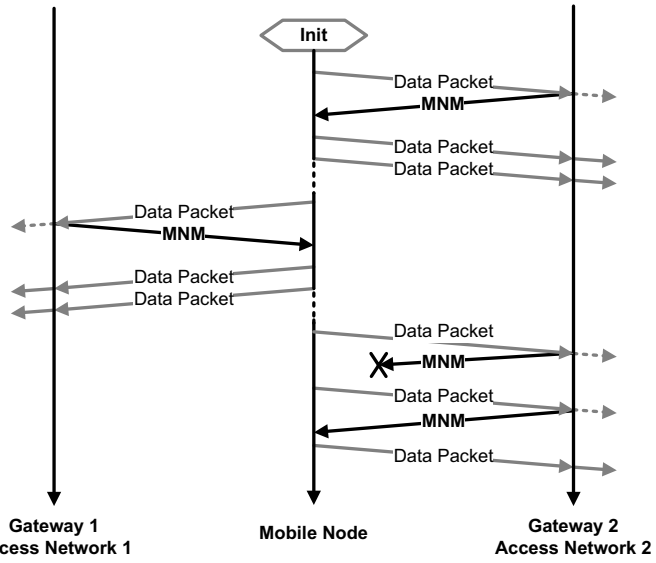

Fig. 2. The gateways inform a mobile node abouts its macro mobility or multihoming using Mobility Notification Messages (MNM).

Protocol Overview: When a node sends packets to the Internet, the gateways detect macro mobility and multihoming of a node by means of the source address of the sent packets and a list of known nodes (see Fig. 2). If the address of a multihomed node is not known or the address of a non-multihomed node does not match the access network, the gateway sends a Mobility Notification Message (MNM) with the configuration information for its access network to the mobile node. A non-multihomed node then adjusts its configuration according to the mobility notification message. A multihomed node includes the new access network in its list of locators. The gateway periodically informs the nodes that some of the sent packets are relayed through the access network the gateway belongs to. Moreover, the gateway translates the network prefix of the source address of the packets going to the Internet to topologically fit the packets to the access network.

Mobility Notification Messages (MNM) are sent from gateways to mobile nodes to inform them about the access networks which are relaying their packets. Mobility notification messages are implemented based on ICMP [12] router advertisement messages according to [13] (see Figure 3). A mobility notification message contains two important information: (i) the notification interval for multihoming; and (ii) the prefix of the access network the sending gateway belongs to. The optimal choice of the notification interval depends on the mobility of the nodes as well on the amount of traffic sent. For moderate mobile networks, we propose to set the notification interval to a default value of 60 seconds.

Macro Mobility Detection and Multihoming Support at the Gateways: Gateways distinguish between mobile nodes supporting multihoming or not by looking at the network prefixes of the nodes addresses. Nodes supporting multihoming

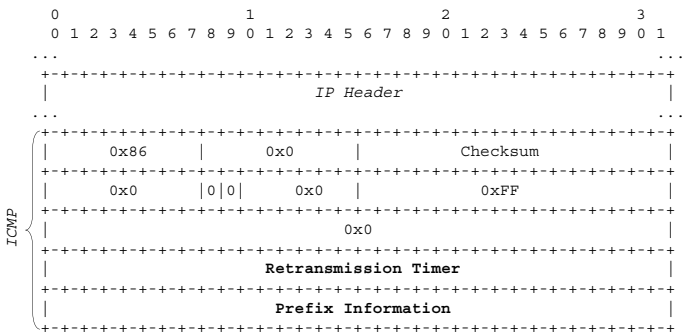

Fig. 3. Mobility notification message format

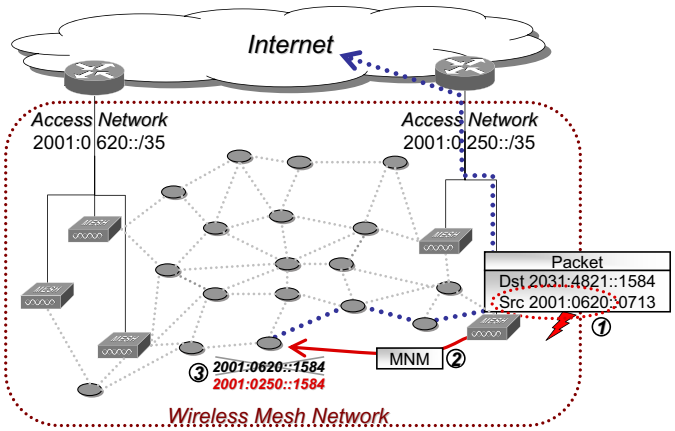

Fig. 4. A gateway detects a packet with a topologically incorrect routing prefix (1). It sends an mobility notification message to the sending node (2). This node then updates its address (3).

always use a link-local address with the prefix *FE80::/64* according to [14] while nodes not supporting multihoming use global addresses.

In the latter case, when the relaying access network of a node changes, the alteration is detected by the gateways of the new access network since the gateways constantly examine all packets they are relaying towards the Internet. If the source address of a packet that is topologically incorrect (i.e., the routing prefix does not match the access network), the gateway sends a *Mobility Notification Message* to the sending node (see Fig. 4).

Processing of packets from multihomed nodes is more complex and requires the gateway to perform two tasks. First, the gateway has to verify if a node has recently been informed that its packets are relayed through this access network. If this is not the case, the gateway sends a mobility notification message to the mobile node to inform it about the actual access network. For reducing the amount of mobility notification messages, the gateway records the node address combined with a timestamp in a lookup table. After a *notification interval*, the gateway deletes the entry and if it is still relaying packets for this node, notifies the mobile node again.

Second, the gateway substitutes the link-local address prefix of the IP source address of the packet with the prefix of the access network it belongs to and forwards the packet to the Internet.

The forwarding algorithm for packets destined to the Internet at the relaying gateways is depicted in Fig. 5.

Handling Mobility Notification Messages at the Mobile Nodes: Handling of mobility notification messages is different at nodes supporting multihoming and those that do not support multihoming. When a multihoming node receives a mobility notification message, it adjusts its address prefix to topologically fit the new access network. Subsequently, it informs about its address change using its IP mobility management protocols. In the case where packets of a node are continuously forwarded over different access networks, multihoming support is an advantage to prevent continuous address changes.

When a multihoming node receives a mobility notification message, it checks if it already is aware of X access network.

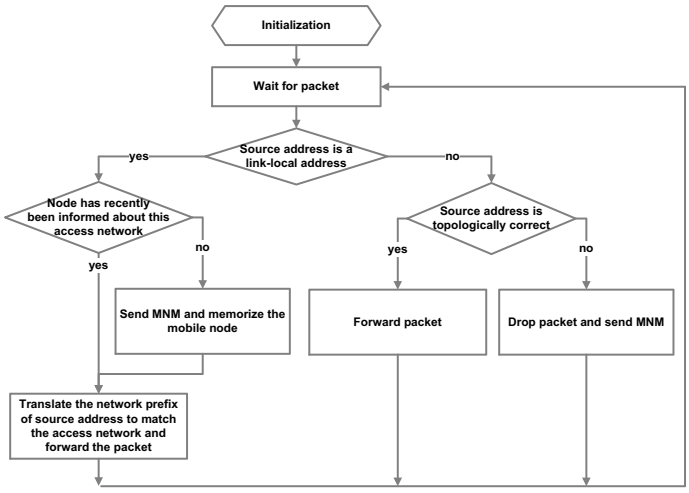

Fig. 5. Algorithm for processing packets destined to the Internet at the relaying gateway.

If this is not the case, it informs its communication peers about its new locator using the multihoming extension of the IP mobility management protocol. Again, we distinguish two methods to detected if an access network does no longer relay packets for a mobile node. First, a communication peer informs a mobile node that it is no longer reachable over a certain access network. Second, a mobile node keeps a list of its relaying access networks with the time stamp of the last mobility notification message received from this access network. From time to time, the mobile node checks its list for outdated access networks. The appropriate choice for the *MNM time out* highly depends on the mobility message notification interval of the gateways, the amount oft traffic sent and on the mobility of a node. For moderate mobile networks, we set the MNM time out to a default value of 3 times the notification interval.

The algorithm for handling mobility notification messages at mobile nodes is depicted in Fig. 6.

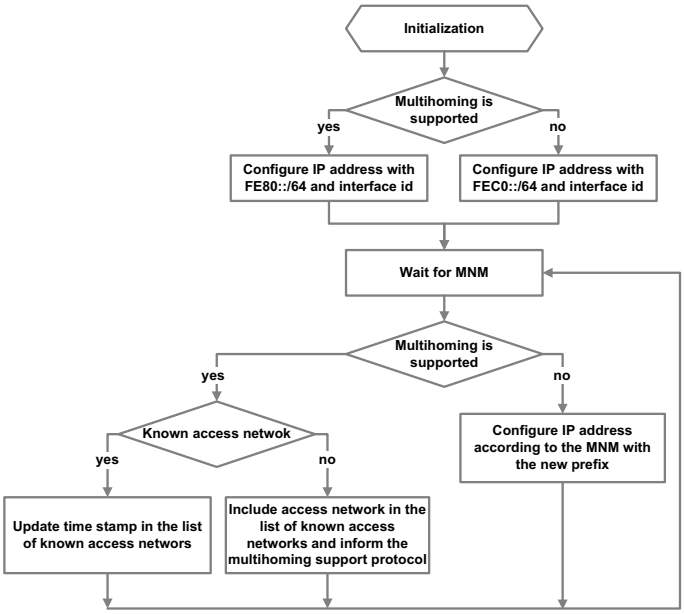

Fig. 6. Algorithm for handling mobility notification messages at a mobile node.

Joining of a Mobile Node: When a node joins a mobile mesh network, it automatically configures its address according to [14] as a link-local address if it supports multihoming, otherwise as a site-local address. These addresses use a specific prefix and an interface identifier as suffix which is derived from the Ethernet address (the prefix *FE80::/64* for link-local addresses and *FEC0::/64* site-local address). Using the automatically configured address, the node immediately participates in the mobile mesh network and no further initialization is required.

IV. Discussion

In this section, we want to briefly discuss two issues coming up when deploying the proposed protocol: supporting of secured connections and making macro mobility transparent to routing protocols.

To support secured connections, only multihomed nodes have to be considered. For those nodes, a problem occurs when IPsec authentication headers [15] are used, since the gateways have to change the (outer) IP header of a packet. Note that IPsec encapsulating security payload [16] is supported since the encryption and authentication is not applied to the (outer) IP header.

Macro mobility is not transparent to routing protocols for wireless mesh networks, because they use the entire IP address as a unique identifier for routing. They do not have any support for nodes which change their address as required for macro mobile nodes. Thus, an address change is treated as a node leave and join which creates unnecessary overhead. A possible solution is that routing protocols for wireless mesh networks only use the interface identifier as identifier for routing. In addition, such a mechanisms also reduces routing overhead and storage requirement.

V. Conclusion and Future Work

There are scenarios in which nodes in a wireless mesh network are unaware of the access network that relays their packets. For these scenarios, we propose a detection mechanism and a notification protocol supporting multihoming which informs the nodes about their macro mobility and thus about the access network they are using.

Currently we are in the process of implementing and evaluating the performance of the proposed protocol in a network simulator as well as on prototype nodes on a large scale test bed.

References

[1] G. Huston, "Architectural Approaches to Multi-homing for IPv6," RFC 4177 (Informational), Sept. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4177.txt

[2] T. Henderson, "End-Host Mobility and Multihoming with the Host Identity Protocol," draft-ietf-hip-mm-04, 2006.

[3] K. U. F. Teraoka, M. Ishiyama, "LIN6: A Solution to Multihoming and Mobility in IPv6," draft-teraoka-multi6-lin6-00, 2003.

[4] M. B. E. Nordmark, "Level 3 multihoming shim protocol," draft-ietf-shim6-proto-05, 2006.

[5] P. M. Ruiz, F. J. Ros, and A. Gomez-Skarmeta, "Internet connectivity for mobile ad hoc networks: solutions and challenges," *Communications Magazine, IEEE*, vol. 43, no. 10, pp. 118–125, 2005, 0163-6804.

[6] R. Wakikawa, J. Malinen, C. E. Perkins, A. Nilsson, and A. J. Tuominen, "Global connectivity for ipv6 mobile ad hoc networks," Internet-Draft, Nov. 2006.

[7] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, and G. M. Jr., "Mipmanet - mobile ip for mobile ad hoc networks," *in MOBIHOC*, pp. 75–85, 2000.

[8] J. M. V.D. Park, "Anycast routing for mobile networking," *Proceedings of MILCOM*, 1999.

[9] R. Baumann and S. Heimlicher and V. Lenders and K. Farkas M. May and B. Plattner, "Field Based Interconnection of Hybrid Wireless Mesh Networks. (*submitted to IEEE Infocom 2007*)."

[10] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), June 2004. [Online]. Available: http://www.ietf.org/rfc/rfc3775.txt

[11] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), May 2006. [Online]. Available: http://www.ietf.org/rfc/rfc4423.txt

[12] J. Postel, "Internet Control Message Protocol," RFC 792 (Standard), Sept. 1981, updated by RFC 950. [Online]. Available: http://www.ietf.org/rfc/rfc792.txt

[13] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461 (Draft Standard), Dec. 1998, updated by RFC 4311. [Online]. Available: http://www.ietf.org/rfc/rfc2461.txt

[14] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462 (Draft Standard), Dec. 1998. [Online]. Available: http://www.ietf.org/rfc/rfc2462.txt

[15] S. Kent, "IP Authentication Header," RFC 4302 (Proposed Standard), Dec. 2005. [Online]. Available: http://www.ietf.org/rfc/rfc4302.txt

[16] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406 (Proposed Standard), Nov. 1998, obsoleted by RFCs 4303, 4305. [Online]. Available: http://www.ietf.org/rfc/rfc2406.txt