

A Macro Mobility and Multihoming Notification Protocol for Wireless Mesh Networks implementing Mobile IP and SHIM6

Rainer Baumann, Olga Bondareva
TIK report 256
Computer Engineering and Networks Laboratory
ETH Zurich, Switzerland
{baumann,bondareva}@tik.ee.ethz.ch

Abstract

Wireless mesh networks provide cost-efficient means to ubiquitous Internet access. Large-scale wireless mesh networks may use multiple access networks. Depending on the routing protocol, a node may not know over which of these access networks it is communicating. In this report, we propose a routing protocol-independent method that allows nodes to (i) determine when they are switching the access network and (ii) to handle switches gracefully or (iii) to support multihoming. In addition, we discuss implementation of the proposed method with Mobile IP as underlying technology to support mobility and Shim6 to support multihoming.

1 Introduction

Internetworking between hybrid Wireless Mesh Networks (WMN) and the Internet is a cost-efficient way of offering ubiquitous Internet access. The interconnection between the WMN and the Internet is provided by gateways connected to an access network.

Usually, large WMNs consist of many gateways belonging to different access networks (see Fig. 1). If a node of the WMN communicates with a node in the Internet, the IP packets are relayed through the WMN to a gateway. When a node moves, then the IP traffic may be handled by another gateway as a result. 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 macro mobility. Depending on the position of a node, it may be the case that packets are handled by multiple gateways at the same time. If these gateways belong to multiple access networks the node is multihomed [1].

For enabling macro mobility and multihoming, there are several IP mobility management protocols and extensions. In this report we suppose that Mobile IP [2] is employed to support mobility. This protocol maintains a fixed proxy (Home Agent), a host that is aware of the current location and address of a node. This enables permanent reachability even with mobile nodes. Since Mobile IP does not support multihoming, we suppose that Shim6 is used for enabling multihoming [3, 4]. Shim6 allows a node to have multiple addresses simultaneously. However, Mobile IP and Shim6 require that a node is aware of the access networks relaying its packets. But this depends on the routing strategy that is used in the wireless mesh network. There are two possible mechanisms:

- (i) 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. In this case, packets are sent to the chosen gateway by means of unicast.

- (ii) An alternative is that 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 a specific one (see [8], [9]). The routing protocol then routes the packets in an anycast manner to one of the gateways.

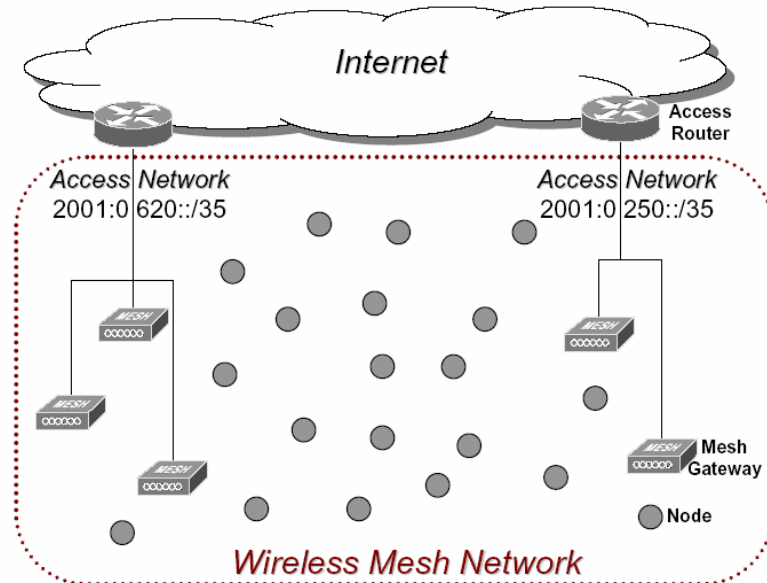


Fig. 1. A wireless mesh network that is connected to the Internet through different access networks.

In the first case, a node knows which gateway relays its packets and thus is aware of its macro mobility. But in the second case the node is not aware of its macro mobility and thus can not use an IP mobility management protocol.

To overcome this shortcoming, we propose a *notification protocol* that is driven by the gateways and is independent of the used routing protocol. A gateway detects the macro mobility of a node by means of the source address of packets from this node. If this address does not match the access network and the node does not use multihoming, the gateway sends a notification message with the configuration information for its access network to the sending node. This node then adjusts its configuration accordingly. If necessary, the node also informs other nodes and its Home Agent about its new address. If the node uses multihoming, the gateway regularly informs the mobile node that some of its packets are relayed through its access network and does a translation of the network prefix to make the packet topologically fit to its access network. If necessary, the node also informs other nodes and its Home Agent about its additional locator address.

Another possibility is to let the gateways and the access networks handle the macro mobility or multihoming of the nodes. In this case, they have to inform the fixed proxy as well as the communication peers of a node. Such a solution requires changes in the IP mobility management protocols and its multihoming extensions. In addition, this solution raises major security-related issues as for example the authorization of gateways by mobile nodes. Due to this we think that this is not an appropriate solution.

The rest of this report is structured as follows. In the following section, we present an overview of Mobile IP and Shim6 to support mobility and multihoming. Then, in section III, we present our solution to handle macro mobility and multihoming. In section IV we address future work and conclude.

2 Overview of mobility support and multihoming using Mobile IP and Shim6

In this section we briefly explain the functionality of Mobile IP - mobility management protocol [2] and Shim6 [3] – a level 3 multihoming protocol. Mobile IP maintains a fixed proxy (Home Agent), a host which is aware of the current location and address of a node. This enables permanent reachability when a node is mobile. MobileIPv6 offers an address change notification mechanism to preserve established transport sessions in the presence of macro mobility.

Since Mobile IP does not support multihoming, we suppose that Shim6 is used to support multihoming. Shim6 allows to take advantage of multiple addresses with minimal impact on the upper layer protocol. The multihoming Shim6 layer is placed after routing related headers in the packet. Applications and upper layer protocols use Upper Layer Identifiers (ULIDs), which shim6 layer maps from different addresses. The shim6 layer maintains the state, called ULID-pair context, between pair of nodes in order to perform this mapping. From the perspective of the upper layer protocols, packets appear to be sent using ULIDs even though address fields in packets might be changed by the shim6 layer.

The combination of Mobile IP and Shim6 allows mobility and multihoming. If there is no need in Mobile IP, Shim6 can be used also to support mobility. In this case, however, a mobile node will not be permanently reachable from the Internet at some fixed address and thus cannot act as a server. Since Shim6 does not maintain a fixed proxy and hides location change from a mobile node. We can define three following scenarios depending on which protocol is used to manage mobility and multihoming:

- I.* Mobile IP is employed to manage mobility; multihoming is not supported.
- II.* Shim6 is used for mobility and multihoming support; mobile node cannot act as a server.
- III.* Shim6 is employed over Mobile IP [4].

In the scenario *III* Mobile IP is used for initial contact between nodes and non-multihomed communications and Shim6 is applied over Mobile IP to make use of multiple addresses transparent for the upper layer protocols. The header extension order is illustrated in Fig. 2. The shim header (see Fig.3) is placed before any endpoint extension headers, but after any routing related header including Mobile IP routing header.

Outer IP header	Shim6 extension header	Mobile IP routing header	ULP
--------------------	------------------------------	--------------------------------	-----

Fig.2 – Extension header order for SHIM6 over Mobile IP.

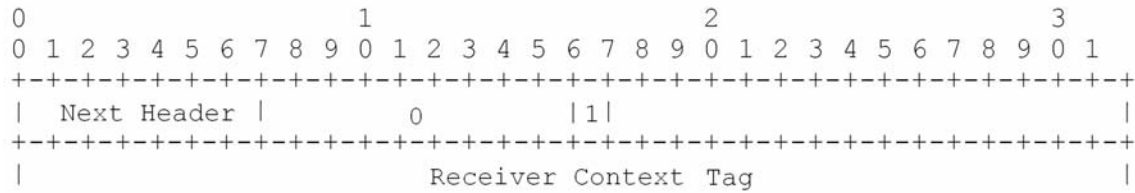


Fig.3 – Shim6 payload extension header

To be explicit, we should also mention the case when corresponding node does not support Shim6 or Mobile IP. In this case packets should be tunneled to the Home Agent. The shim6 context can then be established between the mobile node and its Home Agent.

However, Mobile IP and Shim6 require that a node explicitly knows the access networks over which its packets are forwarded to the Internet. This knowledge allows a node to update its address to topologically fit to the access network relaying its packets and notify its Home Agent as well as its communication peers about its address change. In case of for multihoming, a node informs its communication peer about additional or outdated locators. In the next section we present our notification protocol allowing a mobile node become aware of access networks relaying its packets.

3 Mobility notification protocol

In this section, we describe our notification protocol for IPv6 that allows to handle macro mobility and support multihoming independently of the used routing protocol. First, we give an overview of the proposed protocol and specify a mobility notification message. Then, we explain how gateways detect macro mobility and support multihoming. Following, we specify the handling of mobility notification messages at the wireless nodes and the procedure for node joins. Finally we discuss secure associations and enhancements to routing.

Protocol principles: After initialization a node can start sending packets to the Internet (see Fig. 4). The gateways detect macro mobility and multihoming of a node by means of the source address of the packets and a list of known nodes. 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 wireless node. A non-multihomed node adjusts its configuration according to the mobility notification message. A multihomed node includes the access network in its list of locators and if necessary notifies Home Agent and correspondent hosts. The gateway periodically informs this node that some of its 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 make the packets topologically fit to the access network.

Mobility Notification Messages (MNM) are sent from gateways to wireless nodes to inform them about the access networks which are relaying their packets. Mobility notification messages are implemented using ICMP [10] router advertisement messages according to [11] (see Figure 5). A mobility notification message contains of two important information: (i) the notification interval for multihoming and (ii) the prefix of

the access network the sending router 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 wireless networks, we propose to set the notification interval to a default value of 60 seconds. For integrating security in the mobility notification message, we propose to use the authentication header described in [12].

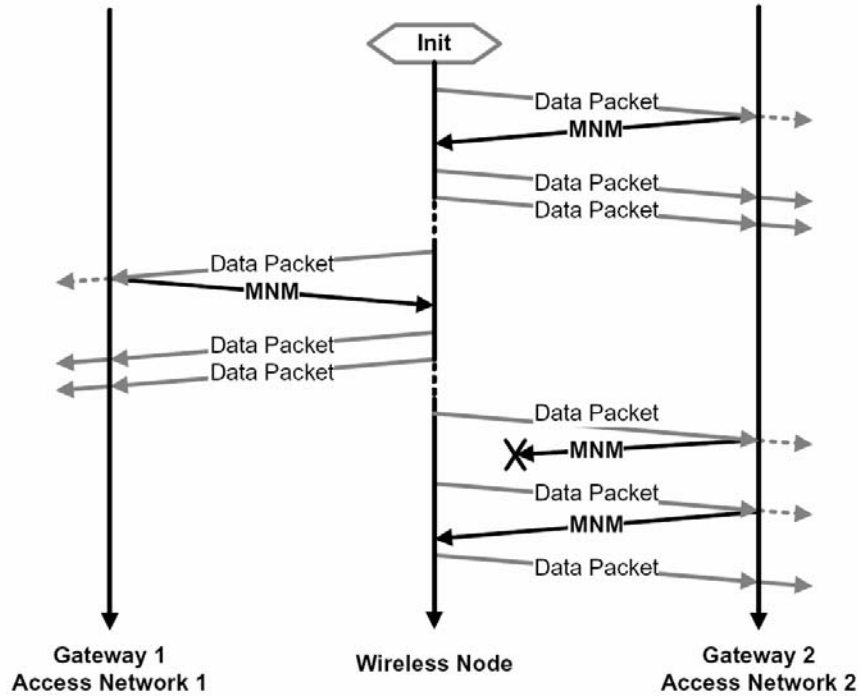


Fig. 4. The gateways inform a wireless node about its macro mobility or multihoming using Mobility Notification Messages (MNM).

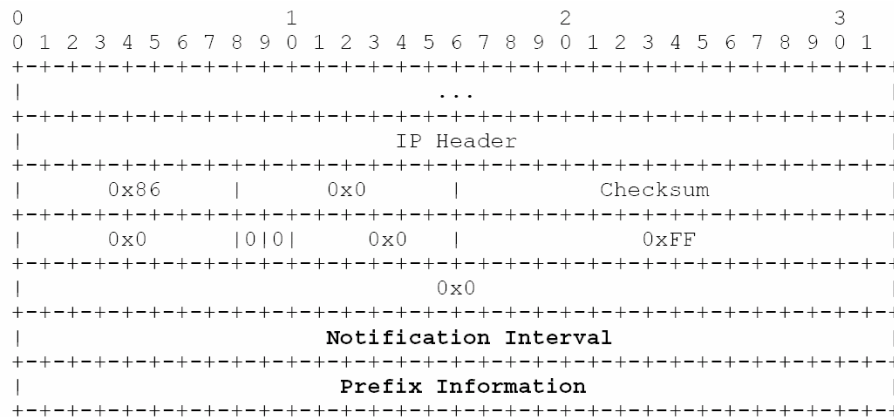


Fig. 5. Mobility notification message format

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

link-local address with the prefix $FE80::/64$ according to [13] while nodes not supporting multihoming use global addresses.

In the second case, when the relaying access network of a node changes, this is detected by the gateways of the new access network because gateways permanently examine all packets they are relaying towards the Internet. If a packet has a source address 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. 6).

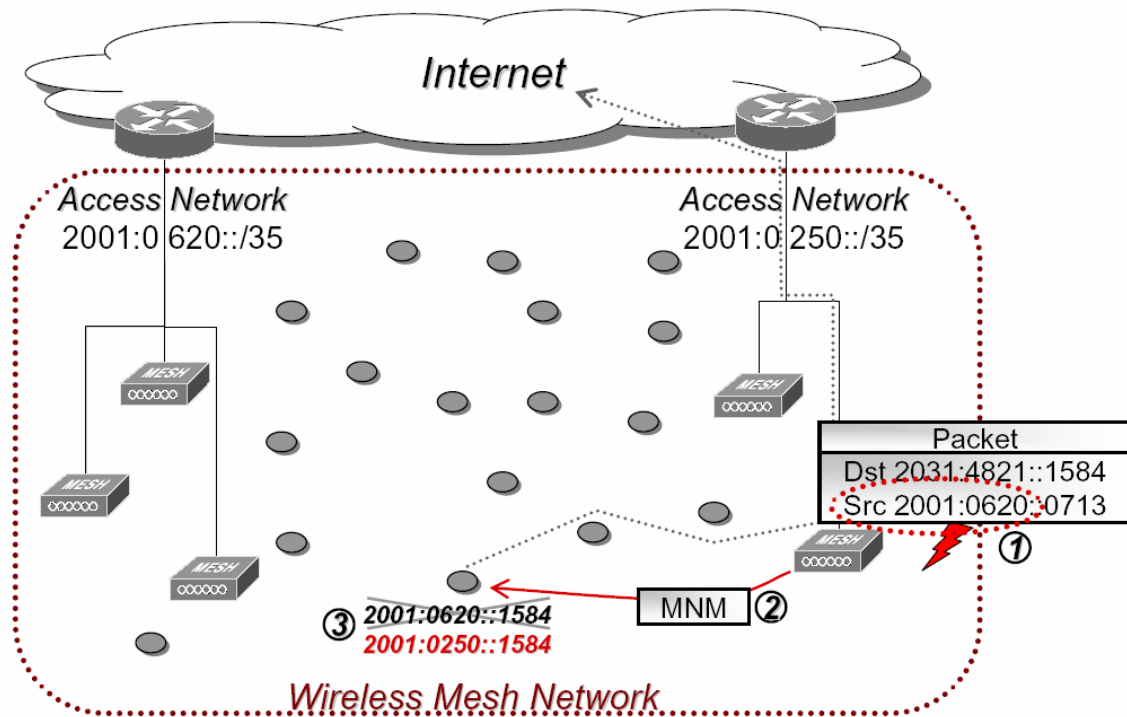


Fig. 4. A gateway detects a packet with a topologically incorrect routing prefix (1). It sends a mobility notification message to the sending node (2). This node then updates its address (3).

Processing of packets from multihomed nodes is more complex. A gateway has first to look up a list if a node has recently been informed that its packets are relayed through this access network. If this is not the case, it sends a mobility notification message to the wireless node to inform it about this access network, which is relaying its packets. For reducing the amount of mobility notification messages sent, the gateway records the node address combined with a time stamp in a look up table. After a *notification interval*, the gateway deletes the entry and if it is still relaying packets for this node, notifies the wireless 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. A detailed processing diagram for packets going to the Internet is depicted in Fig. 7.

Handling Mobility Notification Messages at the Wireless Nodes: Handling of mobility notification messages differ between nodes supporting multihoming and not.

When a node which does not support multihoming (uses only Mobile IP) receives a mobility notification message, it adjusts its address prefix accordingly to topologically fit the new access network. Subsequently, it informs the Home Agent and correspondent hosts about its address change using Mobile IP control messages.

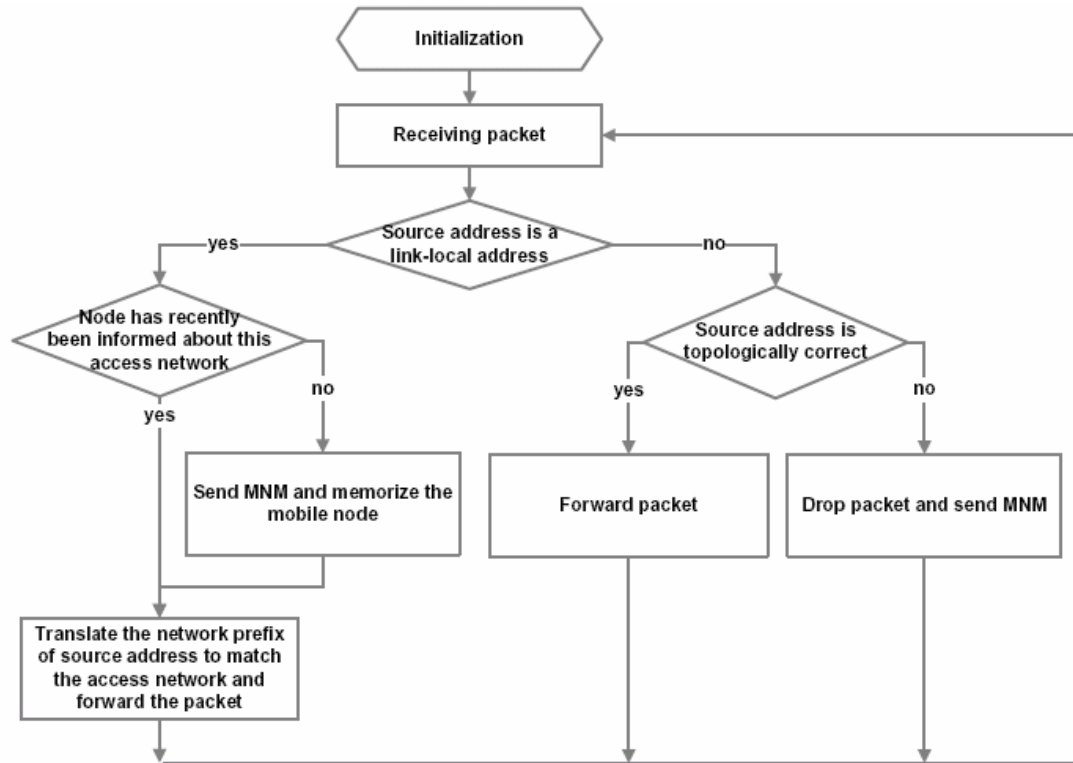


Fig. 5. State diagram for processing of packets destined to the Internet at the relaying gateway

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. If a node supporting multihoming (uses only Shim6 or Shim6 over Mobile IP) receives a mobility notification message, it checks if it already knows that this access network is relaying some of its packets. If this is not the case, it informs its communication peers about its new locator and updates Shim6 context state using Shim6 update messages.

There are two ways how it can be detected that an access network does no longer relay packets for a wireless node. First, a communication peer informs a wireless node that it is no longer reachable over a certain access network. Second, a wireless 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 wireless 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 of 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. A detailed

processing diagram for mobility notification messages at wireless nodes is depicted in Fig. 8.

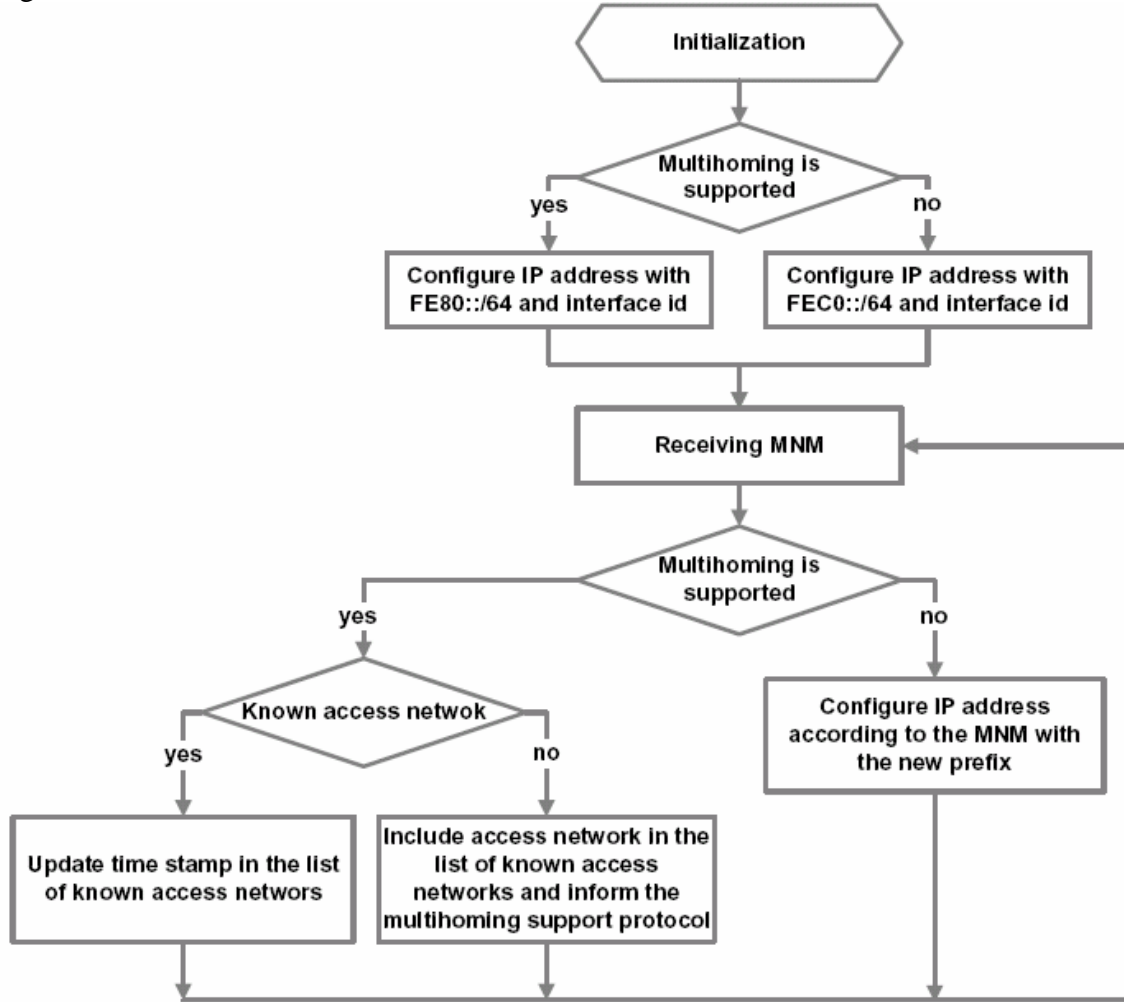


Fig. 6. State diagram for handling mobility notification messages at a wireless Node

Joining of a Wireless Node: When a node joins a wireless mesh network, it automatically configures its address according to [13] 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 wireless mesh network and no further initialization is required.

Supporting secure associations: For supporting secured connections we have to distinguish between multihomed nodes and others. For non multihomed nodes this is no issue, because there are no changes made to packets and the gateways only require access to the source address. For multihomed nodes there is a problem with using IPsec authentication headers [14], since the gateways have to change the (outer) IP header of a

packet. But IPsec encapsulating security payload [15] is supported since the encryption and authentication is not applied to the (outer) IP header.

Routing enhancements: Many routing protocols for WMN 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 by IP mobility management protocols. Thus, an address change is treated as a node leave and join. This creates unnecessary overhead independent of the IP mobility management protocol. A possible solution is that routing protocols for WMN only use the interface identifier as identifier for routing in the WMN. In addition, this also reduces routing overhead and storage requirement.

4 Conclusion and future work

There are scenarios in which nodes of 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. In this report we supposed that Mobile IP and Shim6 are employed to manage mobility and multihoming. Currently we are in the process of implementing and testing the proposed protocol in a test bed.

References

- [1] G. Huston, "Architectural Approaches to Multi-homing for IPv6," RFC 4177 (Informational), Sept. 2005.
- [2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), June 2004.
- [3] M. B. E. Nordmark, "Level 3 multihoming shim protocol," draft-ietfshim6-proto-05, 2006.
- [4] J. Abley, M. Bagnulo "Applicability Statement for the Level 3 Multihoming Shim Protocol (Shim6)" draft-ietf-shim6-applicability-01,2006
- [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] J. Postel, "Internet Control Message Protocol," RFC 792 (Standard), Sept. 1981, updated by RFC 950. [Online]. Available: <http://www.ietf.org/rfc/rfc792.txt>

- [11] 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>
- [12] S. Kent and R. Atkinson, "IP Authentication Header," RFC 2402 (Proposed Standard), Nov. 1998, obsoleted by RFCs 4302, 4305. [Online]. Available: <http://www.ietf.org/rfc/rfc2402.txt>
- [13] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462 (Draft Standard), Dec. 1998. [Online]. Available: <http://www.ietf.org/rfc/rfc2462.txt>
- [14] S. Kent, "IP Authentication Header," RFC 4302 (Proposed Standard), Dec. 2005. [Online]. Available: <http://www.ietf.org/rfc/rfc4302.txt>
- [15] 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>