Poster: A Macro Mobility Notification Protocol for Hybrid Wireless Mesh Networks

Rainer Baumann, Olga Bondareva, Simon Heimlicher, Vincent Lenders, Martin May
Computer Engineering and Networks Laboratory
ETH Zurich, Switzerland

***Abstract*— Wireless mesh networks are a cost-efficient means to provide 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 paper, 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.**

I. 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 (AN).

Usually, large WMNs consist of many gateways belonging to different ANs (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 AN, we refer to this kind of mobility as micro mobility, whereas if they belong to different ANs, we refer to macro mobility.

There are two IP mobility management protocols proposed by the IETF for enabling macro mobility in IPv6: MobileIPv6 [1] and Host Identification Protocol (HIP) [2]. Both protocols maintain a fixed proxy (Home Agent / Rendezvous Server), a host which is aware of the current location and address of a node. This 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. However, these two IP mobility management protocols require that a node is aware of its macro mobility and thus explicitly knows the AN over which its packets are forwarded to the Internet. This knowledge allows a node to update its address and to notify its fixed proxy as well as its communication peers about its macro mobility.

But how does a node become aware of its macro mobility? Typically, this depends on the routing strategy that is used in the WMN. Generally, there are two possible mechanisms: (i) A node uses a gateway discovery protocol to find neighboring gateways (see [3], [4]). 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 [5]). 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 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.

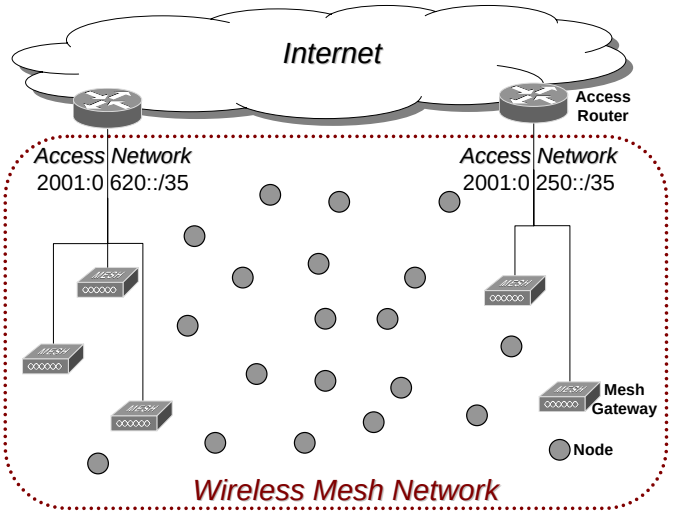

Fig. 1. A wireless mesh network which is connected to the Internet through different access networks.

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, the gateway sends a notification message with the configuration information for its AN to the sending node and the node adjusts its configuration. If necessary, the node then also informs other nodes about its new address.

Another possibility is to let the gateways and the ANs handle the macro mobility 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. 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 optimal solution.

II. Mobility Notification Protocol

In this section, we describe our notification protocol for IPv6 that allows to handle macro mobility independently of the used routing protocol. This protocol enables nodes in a

WMN to use MobileIPv6 [1], HIP [2] or similar IP mobility management protocols. First we describe how macro mobility is detected, then we specify the notification mechanism and the procedure for node joins. Finally, we briefly address security, multihoming and enhancements.

Macro Mobility Detection: When the relaying access network of a node changes, this is detected by the gateways of the new AN 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 AN), the gateway sends a *Mobility Notification Message* to the sending node (see Fig. 2). In order to minimize the number of dropped packets, we propose to also forward packets with invalid source addresses and let the transport layer deal with them.

Mobility Notification Messages (MNM) are implemented using router advertisement messages as specified in [6]. For this purpose, we set the ICMP fields to the values specified in Tab. I. For integrating security in the MNM, we propose to use the authentication header described in [6].

ICMP fields for the mobility notification message

Cur Hop Limit	0
Auto-configuration Flags	0
Router Lifetime	FF
Reachable Time	0
Retransmission Timer	0
Options	Prefix Information

TABLE I

Handling MNMs: When a node receives a MNM, it adjusts its address accordingly and informs about its address change using its IP mobility management protocols. In the case where packets of a node are continuously forwarded over different ANs, multihoming [7] should be applied to prevent continuous address changes.

Joining Node: When a node joins a WMN, it automatically configures its address according to [8] as a link-local address. Such an address consists of the prefix *FE80::/64* and an interface identifier which is derived from the Ethernet address. Using this address, the node immediately participates in the WMN. When it sends its first packets to the Internet, the node is detected and the event is handled as macro mobility.

Enabling Multihoming: In the given context, multihoming refers to the situation in which the packets of a node are relayed through different ANs at the same time. Enabling multihoming for implicit gateway binding poses two additional problems. First, the sending node has to do source address selection independently of the AN over which its packets are relayed. Second, based on the solution for the first problem, the macro mobility detection mechanism at the gateways has to be modified. For example, routing prefix substitution could be deployed at the gateways to solve the source address selection problem. In order to detect macro mobility, the gateways can track the nodes for which they relay packets. Due to space limitations, we are unable to discuss this issue in detail in this paper. For a thorough discussion, we refer to [9].

Enhancement for Routing: 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.

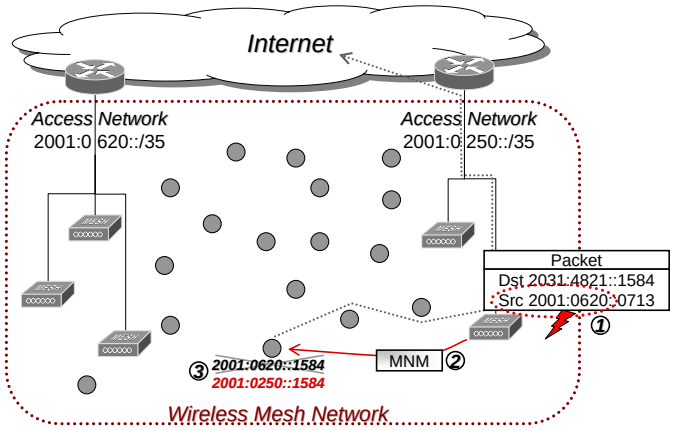

Fig. 2. A gateway detects a packet with a topologically incorrect routing prefix (1). It sends an mobility notification message to the sending node (2). This node then updates its address (3).

III. 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 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 testing the proposed protocol in a test bed. In addition, we are working on a proposal for integrating multihoming in this protocol.

References

[1] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775 (Proposed Standard), June 2004.

[2] R. Moskowitz and P. Nikander, "Host Identity Protocol (HIP) Architecture," RFC 4423 (Informational), May 2006.

[3] 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.

[4] 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.

[5] 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*)."

[6] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461 (Draft Standard), Dec. 1998, updated by RFC 4311.

[7] G. Huston, "Architectural Approaches to Multi-homing for IPv6," RFC 4177 (Informational), Sept. 2005.

[8] S. Thomson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462 (Draft Standard), Dec. 1998.

[9] R. Baumann and O. Bondareva and B. Plattner, "Managing Addressing and Mobility in Hybrid Wireless Access Networks. TIK Report 250," ETH Zurich, Tech. Rep., July 2006.