IPv6 based Mobile Routing

Wolfgang Fritsche
IABG, Einsteinstrasse 20, 85521 Ottobrunn, Germany
fritsche@iabg.de
www.ipv6.iabg.de, www.iabg.de

Abstract: In the past few years the number of mobile Internet users has been continuously growing. Internet access has been provided and used in numerous new scenarios, e.g. in airports, coffee shops, trains, busses, cars, cellular phones, sensor networks, and so on. This mobile access to the Internet faces several new problems, starting from routing and security issues to bandwidth restrictions over narrow band wireless links.

This paper investigates the routing problems of these mobility scenarios, discusses possible IPv6 based approaches to solve them, informs about the current status of solution and the still outstanding issues, and investigates interworking aspects between different mobility scenarios.

Key words: IPv6, Mobility, Routing

1. INTRODUCTION

During the last few years the mobility requirements of Internet users have increased dramatically. The diversity of

- available mobile Internet devices, ranging from laptop computer to PDAs and cellular phones with WAP browsers,
- available radio technologies for carrying Internet traffic, like WLAN, GPRS, UMTS, Bluetooth or satellite networks, as well as
- new scenarios for Internet deployment, like hotels, coffee shops, airports, automobiles or sensor networks

contributes to the high expectations into the market potential of mobile Internet.

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35673-0_28

C. McDonald (ed.), *Converged Networking*

To meet these expectations it is necessary to provide the mobile Internet user a mobile Internet access with similar properties as a fixed one, that is an adequate quality of service and a reasonable level of security. Furthermore the mobility should be transparent to the user and application as much as possible. This latter requirement still places a challenge on today's Internet.

Currently standardization organizations and research institutes are developing routing mechanisms for the Internet, which provide adequate support for mobile users. In this area many solutions are already based on the Internet Protocol version 6 (IPv6) [1]. As part of the mobile routing mechanisms assign different IP addresses to the mobile devices while these are roaming between different points of attachment, IPv6 with its large address space is able to allocate one or more globally unique IP addresses for each mobile device This brings back the end-to-end transparency to the Internet and allows an efficient route aggregation. Furthermore the modular design of IPv6 allows mobile routing mechanisms the insertion of routing information into the IPv6 header. Finally the stateless address autoconfiguration of IPv6 automates and thereby eases the network configuration of mobile devices. All these properties make IPv6 a suitable Internet protocol especially for mobile user.

Currently solutions are developed for the following three mobility scenarios:

- **Host Mobility**, that is a mobile host dynamically changes its point of attachment to the fixed Internet,
- **Network Mobility**, that is a network in motion dynamically changes its point of attachment to the fixed Internet,
- **Mobile Ad hoc Networks**, that is the network itself consists of mobile router and therefore has a dynamically changing topology.

This work first discusses possible mechanisms to support host mobility, network mobility and mobile ad hoc networks, provides an overview of the current status of standardization in this area along with the outstanding issues to be addressed next. Furthermore it investigates interworking aspects between these three mobility scenarios, e.g. a mobile host or network visits an ad hoc network. For the reasons mentioned above this work has been completely based on IPv6.

2. CURRENT STATUS

2.1 Host Mobility

The Mobile IPv6 [3] protocol standardised by the Mobile IP Working Group (MIP WG) of the Internet Engineering Task Force (IETF) supports the mobility of hosts in a way, which is transparent to the user and application. If a mobile host / node (MN) changes its point of attachment to the fixed Internet, it first configures a temporary IPv6 address (care-of address) at the new point of attachment, using e.g. IPv6 stateless address autoconfiguration [2]. The MN informs a Home Agent (HA) located at the MN's home network about this new care-of address together with the MN's home address at its home network. The mapping of the MN's home address to its currently configured care-of address is referred to as Binding, the packet transmitting this Binding from the MN to the HA is called Binding Update. Figure 1 illustrates this mechanism.

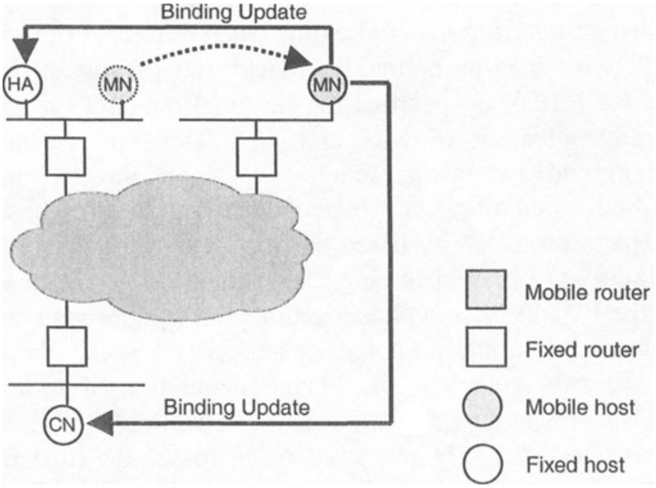

Figure 1 Mobile IPv6 overview

Once the HA has received a valid Binding for a MN, it acts as proxy for the MN at the home network, that is any packet sent by an arbitrary communication partner (correspondent node (CN)) to the MN's home address will be intercepted by the HA and tunnelled to the MN's current location. To avoid the triangle routing from the CN via the HA to the MN, the MN can also send a Binding Update to the CN, that is future packets can then be sent directly from the CN to the MN.

Exactly this route optimisation has been discussed for a long time in the MIP WG. The matter of concern had been the security considerations for sending Binding Updates from the MN to the CN. If an attacker sends malicious Binding Updates to an arbitrary CN, containing its own address as care-of address but the address of someone else as home address, it can easily redirect traffic sent from any CN towards himself. Therefore it is absolutely necessary to authenticate Binding Updates, to be sure, that they are really sent from the MN owning the home address contained in the Binding Update.

The authentication of Binding Updates sent from the MN to the HA can be done using the IPSec protocol. As HA and MN belong to the same subnet and the HA acts as proxy for the MN, it can be assumed, that they anyway have a kind of trust relationship, that is in this case it is possible to exchange offline some keying material to be used later for the IPSec based authentication of Binding Updates.

Between the MN and any arbitrary CN no such trust relationship can be assumed, that is there is usually no way to have any keying material exchanged in advance or to use a common trusted third party. On the other side exchanging keying material online when requested offers the possibility to attackers for man-in-the-middle attacks. To get out of this chicken-egg problem the MIP WG specified the Return Routability mechanism for the mutual authentication of MN and CN. The MN as initiator of this mechanism sends two test packets to the CN, one directly, the other one via the HA, both containing a cookie generated by the MN. The test packet sent via the HA is protected by IPSec on its way between the MN and the HA. The CN replies to both of these packets, again on the direct way to the MN and via the HA. In these replies it returns the cookies generated by the MN and includes additionally cookies generated by itself. From the returned cookies the MN generates the keying material used to authenticate the Binding Updates sent to the CN. This mechanism of Return Routability can be used between the MN and any CN, increases the time for the Binding registration by roughly the round trip time between MN and CN, and prevents against the majority of attacks scenarios.

With this concept of Return Routability the MIP WG addresses the main concern of the IESG, which prevented MIPv6 proceeding to RFC in the past. Return Routability is part of the current version 18 of the MIPv6 Internet draft. Based on this version the WG discusses a number of additional minor issues, expected to be finished soon. Then the MIPv6 draft should be able to proceed to RFC.

2.2 Network Mobility

The scenario of network mobility, that is the scenario of networks changing dynamically their point of attachment to the fixed Internet, has been roughly described inside the MIPv6 draft in the past. Especially in the light of the problems faced by the MIP WG concerning the authentication of Binding Updates between MN and CN, which are expected to be even more complex for complete networks in motion, this part has been removed from the MIPv6 specification and is now dealt with in a separate WG decided to be established soon.

The Network Mobility (NEMO) WG will deal with the mobility aspects of networks in motion [4]. A network in motion is a network, which is attached to the Internet by one or more Mobile Router (MR) and dynamically changes as entire unit its point of attachment. Such a network in motion can consist itself of a hierarchy of subnets, which again can be networks in motion themselves. This case is referred to in NEMO as nested mobility. Networks in motion shall not be confused with mobile ad hoc networks investigated in the Mobile Ad Hoc Network (MANET) WG of the IETF. While in ad hoc networks usually all mobile router constituting the network roam unpredictably and independently from each other, networks in motion always move as an entire unit. Examples for such networks in motion are planes, trains, cars or also Personal Area Networks (PANs).

NEMO will address the mobility aspects of networks in motion in a two step approach:

- The support for the basic network mobility should provide basic reachability to all nodes in the network in motion to allow them session maintenance during IP handovers of the MR. This support should not require any task from the nodes inside the network in motion, but only from the MR itself.
- The support for the extended network mobility should additionally provide means for route optimisation between the network in motion and arbitrary CNs. For this purpose mobility information and tasks can also be provided to nodes inside the network in motion.

As NEMO mainly investigates solutions based on IPv6, it will focus on extensions to MIPv6 for both, basic and extended network mobility support.

One possible solution for a basic network mobility support based on MIPv6 is illustrated in figure 2 [5]. For this solution it is in the first instance assumed, that the network in motion itself consists only of fixed nodes, that is the entire unit of the network in motion is fixed. The addresses of all nodes in the network in motions belong to the same mobile network prefix. The MR has two interfaces, one ingress interface attached to the network in motion and one egress interface attached to the Internet. On the home link of the network in motion the egress interface of the MR is configured with its home address. When the network in motion is moving to a new point of attachment, the egress interface of the MR configures first a care-of address. Like in MIPv6 the MR sends a Binding Update to a HA located at the home link, but in this case the Binding Update contains two Bindings:

- The first Binding contains the current care-of address of the MR's egress interface and as home address the address of the MR's egress interface at the home link.
- The second Binding contains again the care-of address of the MR's egress interface, but the home address field is now filled with the mobile network prefix. To allow this, the format of Binding Updates has to be extended in order to carry prefix information.

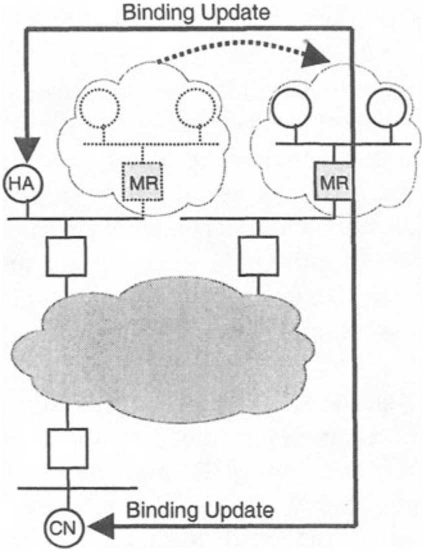

Figure 2 Network mobility overview

Receiving these Binding Updates the HA will act as proxy for the MR's home address and additionally generates a routing entry, enforcing the mobile network prefix to be routed now via the new care-of address of the MR's egress interface. If a packet from a CN destined to a node within the network in motion arrives on the home link, it will be routed to the home address of the MR's egress interface. As the HA acts as proxy for the MR, it intercepts the packet. Looking into its routing table the HA finds an entry generated in consequence of the received Binding Update, that addresses belonging to the mobile network prefix should be routed to the care-of address of the MR's egress interface. Therefore the HA will tunnel the packet to the MR, the MR finally forwards it to the receiving node within the network in motion. Packets originated from nodes within the network in motion will be tunnelled by the MR, using its care-of address as source address in the outer IP header in order to avoid problems with ingress filtering. In order to avoid triangle routing the same Binding Update can be sent from the MR to the CNs communicating with either itself or any node within the network in motion.

In the case of nested mobility the MR of the inner (nested) network in motion will configure a care-of address at its egress interface from the address space of the mobile network prefix of the outer network in motion. Once this has happened, the MR of the inner network in motion can send Binding Updates to his HA and respective CN. The packets of the route optimisation process for the inner network in motion will consequently trigger the MR of the outer network in motion, to also send own Binding Updates to the HA and CNs of the inner network in motion.

Another proposal to solve the problem of networks in motion is described in [6]. This solution is based on the current MIP functionality without any new extensions, but doesn't address route optimisation.

2.3 Mobile Ad hoc Networks

Figure 3 illustrates the mobility scenario of ad hoc networks.

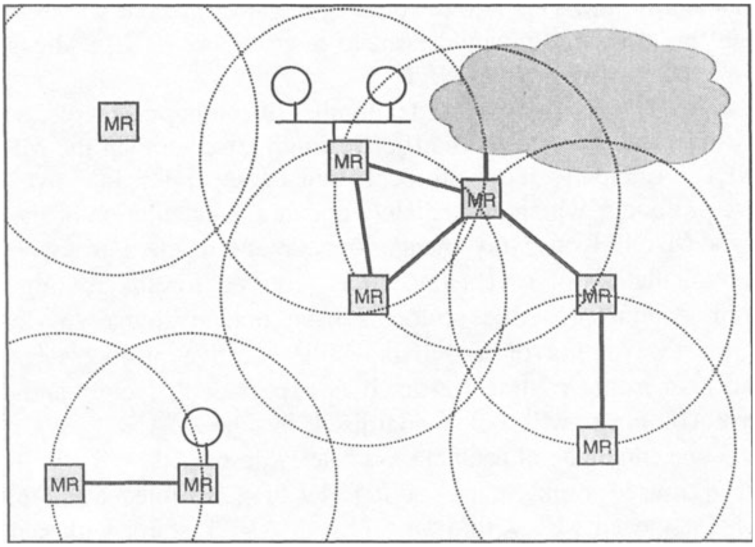

Figure 3 Ad hoc network overview

The dotted circles around the MR should illustrate the covering range of their wireless interfaces. Two MR can only connect symmetrically to each other if they are each in the covering range of their neighbour's wireless interface.

In ad hoc networks MR themselves establish the network topology. As the MR roam unpredictable and independently from each other, the network topology will change dynamically. These changes influence not only the routing topology of an ad hoc network, they also influence the number of MR belonging to an ad hoc network. For example an ad hoc network of n MR can be split due to the movement of some MR into two or more isolated ad hoc networks, without connectivity between them.

Each of the MR can additionally advertise the routes to hosts or networks attached to the MR's non-MANET interfaces. While MANETs can stay self-contained, there is also the possibility of MANETs attached to the Internet. In this case one or more MR of the MANET will act as gateway MR to the Internet.

Concerning the addressing of the MR belonging to the same MANET there are two possibilities:

- Every MR can have its own independent IP address and keeps this address while it roams inside the same or between different MANETs. This kind of addressing results in host routes distributed for all nodes of the MANET.
- All MR in a MANET have IP addresses belonging to the same IP subnet prefix. This allows route aggregation for the whole MANET. In this case a MR would need to re-configure its IP address once it moves into another MANET.

The MANET WG has specified a number of routing protocols, which are able to dynamically establish an efficient routing tree among the MR within a MANET. Principally these protocols can be separated into two classes, proactive protocols, which immediately update the calculation of the routing tree for the MANET once any changes appear, and reactive protocols, which start the calculation of routes once it is required for the routing of user traffic. In general proactive protocols have the advantage to cause less latency for the routing of user data, while reactive protocols cause less overhead concerning routing traffic. It is expected, that one candidate for each protocol class will be standardised by the MANET WG. In the following one candidate of each class is briefly described.

The Optimised Link State Routing (OLSR)[7] represents a proactive protocol. First each MR within an OLSR MANET starts with sending of periodical Hello Messages to its neighbours. In these messages it includes its own interface addresses on all MANET interfaces as well as the interface addresses of all its MANET neighbours received within their Hello

Messages. This allows beside the detection of neighbours itself also the detection of the kind of link symmetry towards them. From its set of neighbours each MR selects a subset as Multipoint Relays (MPRs). With the selection of MPRs OLSR provides an efficient way of flooding. Packets to be flooded are forwarded from the MR not to all neighbours, but only to MPR neighbours. Once the local topology has been detected by a MR and it has selected its MPRs, this local topology information is now flooded within Topology Discovery (TC) Messages throughout the MANET using the MPRs as relays. Additionally each MR with associated hosts or networks attached on its non-MANET interfaces should periodically distribute routing information on behalf of them within the MANET.

Another candidate for a proactive MANET protocol could be Open Shortest Path First (OSPF) for IPv6. The additional extensions OSPFv3 would need therefore are discussed in [9].

The Ad hoc On-Demand Distance Vector (AODV)[8] represents a reactive protocol. In opposite to OLSR AODV doesn't periodically detect its neighbourhood. AODV starts its routing mechanism once packets with user data are received. If the MR has no routing entry for the destination address of the packet, it will start broadcasting Route Requests (RREQs) for this destination address. The range of dissemination of RREQs within the MANET can be controlled by the Time to Live (TTL) value of the RREQs packet. MR forwarding a RREQ packet will also insert an entry for a route back to the originator of the RREQ. Once the RREQ is received from the destination, or from a MR which has an actual route to the destination, a Route Reply (RREP) is sent back by unicast to the originator of the RREQ.

While OSPF for IPv6 has fully integrated IPv6, OLSR and AODV discuss only briefly the integration of IPv6.

3. INTERWORKING ASPECTS

3.1 Mobile Hosts visiting Mobile Networks

One example of interworking of mobile hosts and mobile networks is when the driver of a car attaches his business laptop to the car network. In this case the laptop can be seen as MN with MIPv6 support, the car represents a network in motion.

In this interworking scenario the MN configures a care-of address at its interface from the address space of the mobile network prefix of the network in motion. Next the MN sends Binding Updates to its HA and CNs. As neither HA nor CNs of the MN will have Binding Updates from the MR of the network in motion, the first packets from them to the MN will be sent via the home link of the MR. Receiving these tunnelled packets the MR finally can send its own Binding Updates including the prefix information for the network in motion to the HA and CNs of the MN.

3.2 Mobile Hosts visiting Ad hoc Networks

An example of interworking of mobile hosts and ad hoc networks can be a number of tanks forming a MANET. To some of the tanks laptops are attached as MNs.

For the ·discussion of this scenario it is assumed, that the MANET network always has a gateway to the Internet, over which visiting MNs can reach their HAs at their home network.

One solution to address this scenario is to see MNs visiting a MANET as associated hosts of the MANET MR. In this case the MNs can keep their home address during roaming and therefore don't use their MIPv6 functionality. The drawback here is, that the mechanism of host routes advertised from the MANET MR for their attached MNs will not scale for a high number of frequently roaming MNs.

A more scalable solution is to use a common subnet prefix for all MANET MR and provide this prefix also to visiting MNs. The knowledge of this prefix can be used by the MNs for the following purposes:

- to configure a care-of address using IPv6 stateless address autoconfiguration, and
- to detect the movement of their point of attachment due to the receipt of the new subnet prefix. While MIPv6 doesn't restrict the possibilities for movement detection, most current implementation base this detection on the receipt of IPv6 Router Advertisements (RAs) containing prefix information.

Therefore the roaming of a MN into or out of a MANET sharing one common subnet prefix will be supported by means of MIPv6, while the roaming of a MN inside the MANET between different MR will be supported by means of MANET protocols, that is the respective MR currently having a connection to the MN will advertise the MN's care-of address as associated host.

As this solution is based on the knowledge and use of a common subnet prefix in the MANET, the problem to be solved here is the distribution of this prefix. As RAs containing prefix information are only sent link-local, that is only to next hop neighbours, one possibility would be to allow those RAs to be sent over multiple hops. This would require a modification of the IPv6 neighbour discover protocol (NDP). Another possibility without modification of the currently standardised RA mechanism would be the inclusion of the prefix distribution task inside the MANET specifications themselves. For example in case of OLSR a new Gateway (GW) Message could be specified as illustrated in figure 4. The originator of such a GW Message should always be the MANET MR acting as gateway to the Internet. GW Messages should be flooded throughout the whole MANET and contain the address of the MANET's gateway MR as well as the prefix length in order to derive the subnet prefix of the MANET from the IPv6 address of the gateway MR.

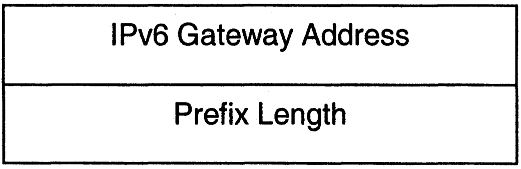

Figure 4 Example for an OLSR GW Message Format

3.3 Mobile Networks visiting Ad hoc Networks

The problem scope of mobile networks visiting ad hoc networks is similar as discussed above for mobile nodes. If there is a mechanism for prefix advertisement throughout the MANET protocol, the MR of the visiting network in motion can detect the new point of attachment, configure a care-of address for its egress interface within the range of this prefix and run the mobility mechanisms specified above for networks in motion.

4. CONCLUSION

There is a huge demand for solutions supporting mobility scenarios. The MIPv6 protocol specified by the MIP WG supports host mobility in IPv6 networks and is close to become an IETF standard. For the specification of solutions for network mobility in IPv6 networks the NEMO WG will be established soon, expected to provide first results based on MIPv6 around spring 2003. The MANET WG specified several solutions to address ad hoc networks. It is expected that one reactive and one proactive solution will be standardised. AODV and OLSR seem to be good candidates for those. All MANET protocols have been mainly specified for IPv4, some first IPv6 consideration have been included recently to some of them. Looking at interworking aspects between these mobility scenarios is still mainly in the research status and needs to be addressed in future by the respective WGs.

IPv6 is able to deal with these mobility scenarios in an efficient way. It's not only the large space of global addresses which allows optimised mechanisms for mobility support, IPv6 stateless address autoconfiguration allows plug & play like configuration of mobile systems, link scoped multicast allows the distribution of control information of MANET protocols in a more efficient way, and IPv6 extension headers and destination options cause less overhead than tunnelling. For these and other reasons solutions for mobility scenarios are recently more investigated for IPv6.

Security and mobility requirements are often conflictive. Most times a trade-off is the only way to accommodate both of them. The huge problems the combination of mobility and security can generate demonstrated the delay of the MIPv6 standard. Nevertheless, more and more attacks against routing protocols could be observed in the recent time, and mobility makes this problem worse. One part of these issues are addressed by the IETF in the recently formed Routing Protocol Security Requirements (RPSEC) WG.

ACKNOWLEDGEMENTS

This work has been partly supported by the European Commission IST 6WINIT project.

REFERENCES

[1] S. Deering, R. Hinden; *Internet Protocol, Version 6 (IPv6) Specification*; RFC 2460; December 1998

[2] S. Thomas, T. Narten; *IPv6 Stateless Address Autoconfiguration*; RFC 2462; December 1998

[3] D. B. Johnson, C. E. Perkins, J. Arkko; *Mobility Support in IPv6*; draft-ietf-mobileip-ipv6-18.txt (work in progress); June 2002

[4] T. Ernst, H.-Y. Lach; *Network Mobility Support Terminology*; draft-ernst-monet-terminology-01.txt (work in progress); July 2002

[5] T. Ernst, A. Olivereau, L. Bellier, C. Castelluccia, H.-Y. Lach; *Mobile Networks Support in Mobile IPv6 (Prefix Scope Binding Updates)*; draft-ernst-mobileip-v6-network-03.txt (work in progress); March 2002

[6] T. J. Kniveton, J. Z. Malinen, V. Devarapalli, C.E. Perkins; Mobile Router Support with Mobile IP; draft-kniveton-mobrtr-02.txt (work in progress); July 2002

[7] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot; *Optimized Link State Routing Protocol*; draft-ietf-manet-olsr-06.txt (work in progress); March 2002

[8] C. E. Perkins, E. M. Belding-Royer, S. R. Das; *Ad hoc On-Demand Distance Vector (AODV) Routing*; draft-ietf-manet-aodv-11.txt (work in progress); June 2002

[9] F. Baker; *An outsider's view of MANET*; draft-baker-manet-review-01.txt (work in progress); March 2002