Interworking RSVP and Mobile IP Version 6

in Wireless Environments[1]

George Fankhauser [a], Stathes Hadjiefthymiades [b], Neda Nikaein [c], Lorraine Stacey [d]

[a] ETH Zürich, Switzerland , <gfa@acm.org>

[b] University of Athens, Greece, <shadj@di.uoa.gr>

[c] Eurecom, France, <nikaein@eurecom.fr>

[d] Lucent Technologies, UK, <lstacey@lucent.com>

Abstract

This paper gives an outline and solutions to the problem of running RSVP signalling in Mobile IP (Mobile Internet Protocol) networks using optimised routing. First, we discuss a basic solution to this problem. By modifying RSVP at mobile and correspondent nodes to become aware of MIPv6 addressing, we provide a simple repair that allows RSVP flows to be established between the fixed network and mobiles. Then, by adding optional objects to RSVP messages, a performance enhancement is proposed to make handovers smooth and seamless. A different technique to enhance performance is called flow extension which provides flows with fixed flow-ids from the correspondent node into the wireless access network at the expense of forwarding traffic inside the access network, whenever the mobile node moves.

We conclude that the basic solution is a requirement in order to make MIPv6 and RSVP interoperable. For well performing and uninterrupted operation we strongly recommend one of the performance enhancements that support fast re-establishment or preservation of resource reservations when mobile nodes move.

1. Introduction

Wireless access to the Internet is becoming more and more popular due to the rapid spread of wireless LANs and other wireless access technologies (IEEE 802.11, CDPD, GPRS, etc.). Mobile IP (MIP) [Per98a] could become a common platform for mobile access (regardless of the underlying access technology), providing solutions to the many security, routing, and addressing problems. More traditional services like telephony, radio and TV broadcasting, and other new Internet applications that require more than best-effort service are increasingly being carried on the Internet. Mobile users also want to enjoy multimedia and other real-time services. Therefore, it is important to design MIP to interoperate seamlessly with protocols that provide real-time services in the Internet. This paper focuses on issues of MIPv6 [Joh98] and RSVP [Bra97] interoperability, more precisely on the operation phase where optimised routing between fixed and mobile hosts is used. We apply our considerations to MIPv6 because it uses route optimisation by default. However MIPv4 may also use this technique [Per98b].

2. Problem statement

2.1 Unicast Scenario

MIPv6 uses optimised paths between a mobile node (MN) and its correspondent nodes (CN). Routing of packets via the Home Agent (HA) is typically only a transient phase. After the first packets from CN arrive at MN a binding cache update message is sent back to the CN to initiate optimized routing. Here, we will discuss the case where the MN has one or more packet flows using the direct, optimised route between the MN and CN. When an MN moves, the optimised route between the MN and CN will change in addition to the MN's care-of address (COA). Both the route and COA change affect the operation of RSVP. The addressing using optimised routes is shown in figure 1 below. Since establishment of optimised routing is usually a short procedure we do not look at the phase where packets travel via the

[1] A detailed and more technically oriented version of this text can be found in the Internet Draft [Fan98].

HA. However, it has to be noted that the operational changes to protocols described in this document should be initiated as soon as optimised routing is established in order to prevent long reservation setup times (i.e. we should not wait for the next RSVP period, cf. also section 3.1.1).

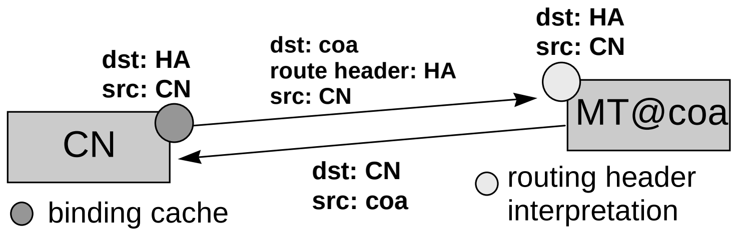

Figure 1: Addressing used in optimised routing

RSVP PATH messages are sent end-to-end (E2E) while RESV messages are sent hop-by-hop. When the CN is a sender it will transmit a PATH message where the address details are based on the MN's home address. However, the outer IP header details will be modified by the MIPv6 binding cache to contain the MN's COA as the destination address. Even more importantly, to ensure PATH and RESV messages follow the same route, the PATH messages contain a RSVP_HOP object which collects the address of each outgoing interface the message traverses. The CN and intermediate routers will each determine the outgoing interface based on the MN's home address. However, the packet will actually be routed based on the MN's COA. Thus, when the PATH message reaches the MN the routing information stored in the RSVP_HOP object will not be consistent with the route followed as shown in figure 2. Hence, RESV messages can not be routed back to the CN and therefore RSVP state will not be created between the MN and the CN. Additionally, RESV messages sent back from the MN reference the home address of the MN as the flow's destination in the SESSION object. Again, this is not the real flow-id of the flow's packets, it should rather reference the MN's COA.

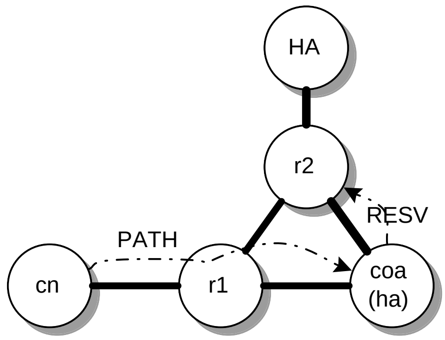

Figure 2: Inconsistent hop-by-hop forwarding of RESV messages

For the unicast case, the problem of this flow-mismatch occurs when the CN is the sender. When the MN is the sender, the PATH message will contain correct routing information when it reaches the CN because the MN directly addressed it to the CN. Hence, the RESV message can be forwarded correctly along the reverse path. Also, the RESV message's SESSION object sent by the CN contains correctly its own (fixed) address as the flow's destination. However, the PATH messages also contain the sender's address (MN) in the SENDER_TEMPLATE object. This address would be normally the home address of the MN and has to be changed to its COA. Solutions to these 'change of route' and 'flow-mismatch' problems are discussed in this paper.

Another important issue is that when the MN moves to a new subnet its COA changes. In standard RSVP, state information is based on the MN's home address. However, the data packets this state needs to apply to will be addressed with the MN's COA. Hence, there is an issue of matching RSVP flow state with the data packets belonging to that flow at intermediate routers. Yet, another difficulty with MIPv6 is its applicability to wireless environments where the MN moves to new subnets in real time. In wireless environments, the speed of re-routing is of major concern. The objectives are to minimise the loss of packets, and restore the E2E RSVP state as quickly as possible.

2.2 Multicast Scenario

In the multicast case, there are two options for MN to receive data. The first option is through its HA. In this case, the HA is also a multicast router. The HA tunnels the multicast packets to the MN. The second option is for the MN to join its groups directly in its foreign network. This option allows the MN to receive the multicast packets directly without HA involvement. Only the second option is studied here.

Let's consider the case where the CN sends multicast data and at least one of the receiver's is a MN. An RSVP session is identified by the triple destination address, protocol id and optionally destination port. The destination address of a multicast group remains fixed regardless of the mobility of its receivers. In other words, the MN's exact address and its mobility have no impact on the multicast group address. Therefore, an MN making a handover to another network can simply be considered as a new node joining the group. That is, each time the MN moves to a new subnet it must leave and re-join the multicast group.

Now, we consider the case where the MN sends multicast data. IP unicast routing protocols depend only on the IP destination address. Some multicast routing protocols such as DVMRP [Wai98] and MOSPF [Moy94] build a multicast tree per source. These routing protocols construct the multicast tree depending on the source and the destination addresses. Other algorithms like CBT [Bal97] build a single shared tree per group. These protocols use only the IP destination address for packet forwarding. Using the home address as the IP source address of the datagram leads the routers executing DVMRP or MOSPF to expect the datagram from the link used to reach the MN's home address. Therefore, sending multicast traffic in a foreign network using the MN's home address as the IP source address means that these routers receive the traffic via unexpected links. DVMRP drops such datagrams because it expects the packet to arrive to the router on the shortest path from the router to the MN's home address. MOSPF forwards the traffic based on an incorrect information. In both cases, some destinations may not be reached. In order to overcome such routing problems, the MN's care-of-address should be used as the source address.

3. Possible Solutions

3.1 Mobility Enhanced RSVP

3.1.1 Solving the Routing Problem at End-Nodes

One possible solution to the problem of correctly routing RSVP messages between CN and MN is to modify the RSVP daemon at the CN and MN to operate on the MN's COA instead of its home address. The RSVP daemon could learn the COA by consulting MIP’s binding cache. This means that RSVP state would be created based on the COA, and thus, the path that traffic actually follows. There are two ways that the COA can be obtained. One option is to modify MIP to provide an interface that allows the RSVP module to look up the COA of a MN. An alternative is to modify MIP at the CN and MN only. In this case the MIP module needs to become RSVP aware and swap the home address in the PATH and RESV messages SESSION objects with the MN’s COA (among other fields). We recommend the implementation of an interface in MIPv6 which must be used by the RSVP daemon. As discussed below, this interface may also be extended for triggering PATH messages when MNs change their location. This option is shown in figure 3.

3.1.2 Solving the Routing Problem at Intermediate Nodes

An alternative approach involves changing the RSVP implementations at routers. Changes are not required at CNs and MNs. Outer header address information is passed up to the RSVP daemon at each router (outer header means the IP header transporting the RSVP messages, i.e., the whole packet and not only the payload is forwarded to the RSVP daemon). This allows the RSVP daemon in each intermediate router to learn the mapping between the MN's home address and current COA. The RSVP daemon should then base its calculation of the RSVP_HOP and filters on the COA. Given the router RSVP daemon maintains a mapping between the home and COA when the COA changes the router will still recognise the RSVP messages and traffic as belonging to the same reservation. Since we can’t control the signalling path along a global network with many providers this approach should be avoided.

3.1.3 Performance Enhancements

One minor disadvantage of the previous approaches is that when the MN moves and thus, obtains a new COA, all of the intermediate routers will assume this is a new RSVP flow. Hence, there may be situations where the new reservation is denied because the old reservation is still active and consumes resources. This problem could be overcome by introducing a new RSVP object to the RSVP messages the MN sends (that is, if the MN is a receiver, it will place the RSVP object in the RESV message). This would allow intermediate routers to recognise the reservation is the same even though the COA has changed. If some or even all intermediate routers do not recognise this RSVP object, this solution will still work. At those routers that don't understand the RSVP object, the RSVP state with the new COA will be treated as a new independent flow and the previously reserved flow expires later.

If the home address was kept as the destination address, and the COA was stored in the new RSVP object this solution would require all intermediate routers to understand the new RSVP object instead of just changing the CNs and MNs and treat the new RSVP object as an option.

Another issue is the time required to modify the RSVP state so that traffic flows along the optimal path to the MN's new COA. In standard RSVP operation, PATH and RESV messages are transmitted periodically. Hence, there can be a significant delay between the MN's COA change and the transmission of the next PATH message. This delay can be avoided by having the arrival of a binding update message at the CN, trigger (through some interface) the transmission of a PATH message.

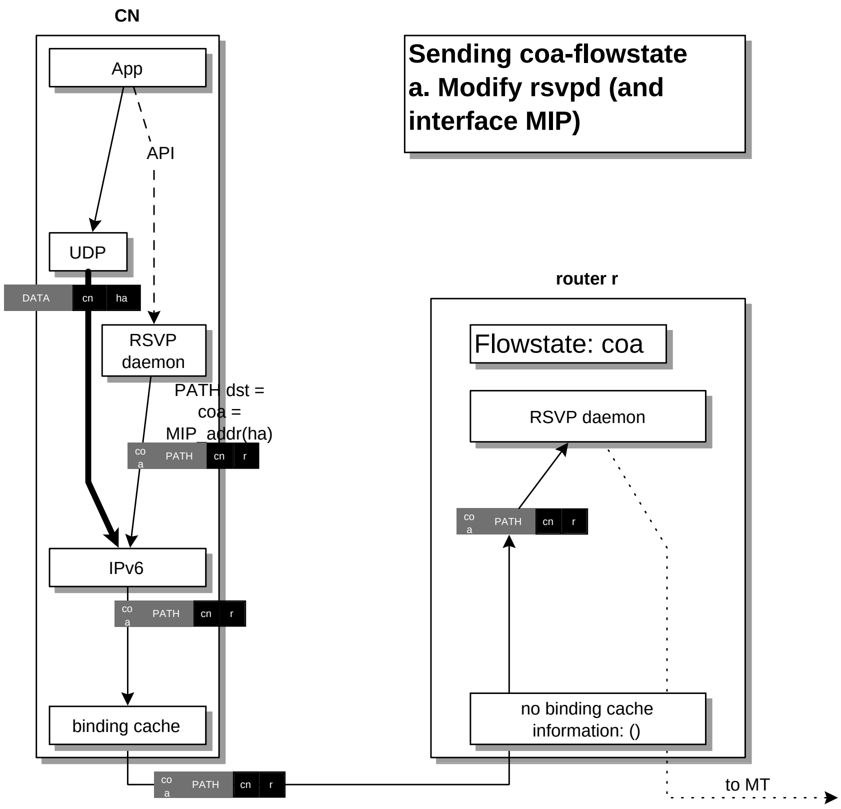

Figure 3: Interfacing MIPv6 and RSVP

3.1.4 Use of IPv6 Flow Label

One could argue that the mechanism described above is not required, since IPv6 flow labels (in conjunction with the source IP address) uniquely identify the traffic flow. If non-zero flow labels are employed it is still possible to identify the traffic flow. However, this won't solve the routing problem of PATH messages. Moreover IPv6 flow labels are optional and hence they can often be zero. If this is the case the flow-id mismatch problem still exists. Furthermore, if the flow-id is created by hashing on the destination address, it may also change when the COA changes.

3.1.5 Multicast Support

The same approach can be used to resolve the problem of multicast reservation when an MN is a sender. In this case, we can also use the care-of-address in the IP source address field of the SENDER_TEMPLATE. Therefore, the RSVP_HOP object of the PATH message is calculated correctly. However, this can cause the intermediate routers to consider the MN as a different source. In order to overcome this problem, we use the same approach as described above (Section 3.1.2). We add a new RSVP object to the PATH message which contains the MN's home address.

3.2 Flow Extension

3.2.1 Solution Description

This section describes an alternative approach for the efficient operation of RSVP on top of MIPv6. This approach proposes an alternative to the use of new RSVP objects for the fast update of E2E RSVP connections. It mainly refers to the time periods following the occurrence of handovers. It is also assumed that, prior to handovers, flows have been established between the CN and the MN using the approaches discussed in Section 3.1.

When an MN attaches to a new subnet and acquires a new COA, the MIP-capable router in this subnet must intercept and suppress the MIPv6 binding update message sent to the CN (we use the term MIP-router here for a router serving wireless access networks and performing the flow extension tasks). This prevents the CN from updating its Binding Cache. This strategy is not applied to the Binding Update sent to the former MIP-router. This information can be used to forward best effort traffic destined to the old location of the MN, to its current location (through the use of an IP tunnel between former and current MIP router). The MN is then capable of receiving datagrams destined to its current IP address as well as the previous IP address. For best effort traffic destined to the MN, the previous IP address should be used. This packet forwarding technique is an enhancement to support loss-less handovers [Had98].

Prior to or during the relocation of the terminal, the old MIP-router also extends the existing RSVP flows to the new MIP-router. This task is performed by a mobility management (MM) entity operating within the router. The extension of downlink (CN $\rightarrow$ MN) flows is performed by the old MIP-router while the uplink flows (MN $\rightarrow$ CN) are handled by the new MIP router. For this last step, the new MIP-router needs to receive the characteristics of existing flows from the old router. For this task, specialised signalling between MIP-routers (MM entities in particular) is introduced. The elongation of flows avoids their invalidation caused by changes in the IP addresses of connection endpoints.

The proposed elongation of the CN-MN path causes the route of the communication to be sub-optimal and, consequently, imposes additional, but limited, transmission delays. It was shown that consecutive elongation (increased sub-optimality) will be needed rarely, as the number of inter-subnet HOs (changes in addresses) is very small during the lifetime of connections in a CPN [Vee97]. Most relocations will result in attachments of the MN to base stations in the same subnet (intra-subnet HO). Such mobility events can be handled at the local addressing-level without affecting the path beyond the router. This elongation of data paths has been adopted in WATM technology for the handling of connections during handovers [Ach97], [Agr96], [Had98].

It is also possible to suppress the binding update messages at the MN without considerable modifications to its MIPv6 module. Such approach preserves bandwidth at the radio interface and reduces the complexity of MIP routers. One additional advantage of this alternative is that it does not cause disruptions in IP communication if the Binding Update message is included (as Destination Option header) in IP packets having, besides headers, standard payload data such as TCP/UDP. Disabling the transmission of Binding Update messages at the MN is also adopted in the MRSVP approach [Tal97].

Lastly, we are considering how the extension of RSVP flows could be accomplished with existing protocols, (i.e., RSVP, MIPv6, IP encapsulation). RSVP operation over IP tunnels [Ter98] provides a good basis for the implementation of the proposed scheme. The old MIP-router uses regular IP tunnels for forwarding BE traffic and RSVP tunnels for handling the extension of RSVP flows. The old MIP-router serves as the RSVP tunnel entry point in the downlink direction while the new MIP-router is the tunnel exit point (roles are inverted in uplink communication). The tunnel session is a separate RSVP session between the involved routers. Its characteristics are dictated by the characteristics of the flows that need to be extended. The original session (CN $\rightarrow$ MN / MIP-router) views the tunnel as a single communication link. The PATH and RESV messages of the E2E session are encapsulated at one tunnel end-point and decapsulated at the other. The E2E session and the tunnel session are associated at the entry/exit points of the tunnel. The tunnel may encompass one or more RSVP-capable nodes.

The overall scheme is based on the assumption that the new MIP-router is aware of the existence of RSVP flows and thus, suppresses only the binding update messages for active RSVP flows When the entire set of RSVP flows is terminated, the new MIP-router allows the propagation of the binding update signal to the fixed network. This restores the optimal communication between the MN and the CN regarding best effort traffic.

3.2.2 Multicast Support

As mentioned before, if the MN, which is the receiver of multicast data, changes its subnet, it must rejoin its groups in the new subnet. Now, if the new subnet already has members of the MN's groups with the same reservations, the MN can receive the data without any delay. If this is not the case, the MN can receive data from its old MIP-router by using an RSVP tunnel. The new MIP-router knows about the MN's group list and also about the presence of groups and their reservation style in its local network. Therefore, instead of trying to graft a path to the multicast tree, the new MIP-router asks the old MIP-router to forward the traffic destined to this group via an RSVP tunnel. The same thing happens, if the new MIP-router has a member of the group but not with the specified reservation style. Now, if the MN is the sender of the multicast traffic (uplink direction), an RSVP tunnel should be used to reach the old MIP-router.

4. Conclusions

In this paper we have identified a series of fundamental problems associated with the interworking of RSVP and MIPv6. We have proposed several solutions involving changes at various components of the considered architecture (e.g., routers, nodes). Besides the basic solution we proposed performance enhancements using optional RSVP objects to identify flow changes and a technique called flow extension to prevent flow changes.

For future work we will also consider other QoS provisioning schemes for the Internet, such as diffserv, and their influence on Mobile IP and QoS signalling. Furthermore we will also extend our studies to the upcoming proposals for hierarchical mobile routing.

References

[Ach97] A. Acharya, J. Lin, B. Rajagopalan, and D. Raychaydhuri, “Mobility Management in Wireless ATM Networks”, IEEE Communications Magazine, November 1997.

[Agr96] P. Agrawal, E. Hyden, P. Krzyzanowski, P. Misthra, M. Srivastava, and J. Trotter, “SWAN: A Mobile Multimedia Wireless Network”, IEEE Personal Communications , April 1996.

[Bal97] A. Ballardie, “Core Based Trees (CBT version 2) Multicast Routing - Protocol Specification”, RFC 2189, September 1997.

[Bra97] R. Braden, L. Zhang, S. Berson, S. Herzog, and S. Jamin, “Resource Reservation Protocol (RSVP) - Version 1 Functional Specification”, RFC 2205, September 1997.

[Had98] S. Hadjiefthymiades, S. Paskalis, G. Fankhauser, and L. Merakos, “Mobility Management in an IP-based Wireless ATM Network”, proceedings of ACTS Mobile Summit '98 , June 1998.

[Joh98] D. Johnson and C. Perkins, “Mobility Support in IPv6”, Internet Draft, draft-ietf-mobileip-ipv6-06.txt, work in progress, August 1998.

[Moy94] J. Moy, “Multicast Extensions to OSPF”, RFC 1584, March 1994.

[Nik98] N. Nikaein and C. Bonnet, “Wireless Multicasting in an IP Environment”, proceedings 5th Intl. Workshop on Mobile Multimedia Communication MoMuc '98 , October 1998.

[Per98a] C. Perkins “Mobile Networking Through Mobile IP”, IEEE Internet Computing , January 1998.

[Per98b] C. Perkins and D. Johnson, “Route Optimization in Mobile IP”, Internet Draft, draft-ietf-mobileip-optim-07.txt, work in progress, August 1998.

[Tal97] A. Talukdar, B. Badrinath, and A. Acharya. MRSVP: A Resource Reservation Protocol for an Integrated Services Packet Network with Mobile Hosts. Technical report DCS-TR-337, Rutgers University, 1997.

[Ter98] A. Terzis, J. Krawczyk, J. Wroclawski, and L. Zhang, “RSVP Operation Over IP Tunnels. Internet Draft”, draft-ietf-rsvp-tunnel-03.txt, work in progress, August 1998.

[Vee97] M. Veeraraghavan and G. Dommety, “Mobile Location Management in ATM Networks”, IEEE JSAC, October 1997.

[Wai98] D. Waitzman, C. Patridge, and S. Deering, “Distance Vector Multicast Routing Protocol”, RFC 1075, November 1988.

[Fan98] G. Fankhauser, S. Hadjiefthymiades, N. Nikaein, and L. Stacey, “RSVP Support for Mobile IP Version 6 in Wireless Environments”, Internet Draft, (draft-fhns-rsvp-support-in-mipv6-00), Mobile IP Working Group, November 98.