Mobility Management in an IP-based Wireless ATM Network

Stathes Hadjiefthymiades[1], **Sarantis Paskalis**[1], **George Fankhauser**[2], **Lazaros Merakos**[1]

[1] Communication Networks Laboratory, Dept. of Informatics, University of Athens, Athens, Greece
(shadj | paskalis | merakos)@di.uoa.gr

[2] Computer Engineering and Networks Laboratory, ETH Zurich, Zurich, Switzerland
gfa@acm.org

Abstract: Traditionally, mobility support in IP was not designed for wireless systems but rather for relocation of wired terminals in a new sub-network. With new wireless technology, the question arises how mobility for such systems can be supported on the Internet. The extension of a wireless ATM access network to support native IP access with IP-based mobility management is described. Using standard protocols, such as Mobile IP, RSVP, and IFMP, a reasonable solution can be designed with only minor extensions or modifications to these protocols.

1. Introduction.

The Wireless ATM Network Demonstrator (Magic WAND) project, implemented in the context of the ACTS Programme, introduces ATM technology in wireless customer premises network environments (WATM) thus rendering mobile terminals capable of handling multimedia traffic. In this framework, IP applications are supported through LANEv1. Mobility management is performed by specialised entities in both the fixed network (Control Station, CS) and the Mobile Terminal (MT). Such entities communicate with each other using the proprietary MMC (Mobility Management and Control) protocol [Kal96], which relies on the Signalling ATM Adaptation Layer (SAAL) for the assured transfer of messages. Conventional Call Control (CC) is carried out by ATM Forum UNI 3.1 compliant entities placed in the MT as well as the CS. Communication between them is also based on SAAL.

In this paper, we outline the efforts undertaken by the WAND consortium's extension work for the specification and design of a wireless ATM LAN, exclusively intended and optimised for IP traffic, and focus on the management of terminal mobility (an in-depth study of other issues can be found in [Ala98]). The IP orientation of our work is justified by the immense growth in the use of IP applications, experienced over the past years. The provision of Internet services over ATM links has been studied for quite a few years. However, in the WAND case, extra challenges, such as the wireless nature, support for QoS guarantees and terminal mobility, need to be dealt with. The design of the pursued IP-based WATM architecture is based on emerging standards such as Ipsilon's IP routing [New97], Mobile IPv6 [Joh97] and IPv6 [Dee95].

2. Architecture, Protocol Stacks and Functional Entities.

This section provides a brief overview of the considered network architecture, the protocol stacks of the various components as well as the functional entities needed to support them. The core components of the wireless architecture considered here are Mobile Terminals (MT) and Access Points (AP). APs are attached to Mobile IP routers and form together the access network. Mobile IP routers are interconnected to other switches of the backbone network and thus provide access to fixed or wireless terminals. In this architecture, in contrast to the WAND pilot, the rather slow ATM signalling protocols were substituted by RSVP (Resource Reservation Protocol) and IFMP (Ipsilon Flow Management Protocol). RSVP [Bra97] serves in the case where QoS guarantees are explicitly requested by terminals for specific connections (this scenario results in the end-to-end establishment of dedicated, cut-through VCs). IFMP conveys VC allocation requests which can be triggered either explicitly, through the use of RSVP, or by the flow classification mechanism introduced in the Mobile IP routing technique (which also results in cut-through, switched connections). As discussed in [Bas97], VC allocation requests may also be piggybacked into the RSVP PATH messages. In the proposed architecture, provision is also made for Best-Effort (BE) connections, without QoS requirements. All BE connections pertaining to the same MT are routed on the same default VC and are scheduled FIFO as in traditional IP routers. Each Mobile IP router is controlled by a workstation (Switch Controller, SC), which performs flow classification and routing of BE connections in addition to low-level switch management (by means of GSMP [New96]).

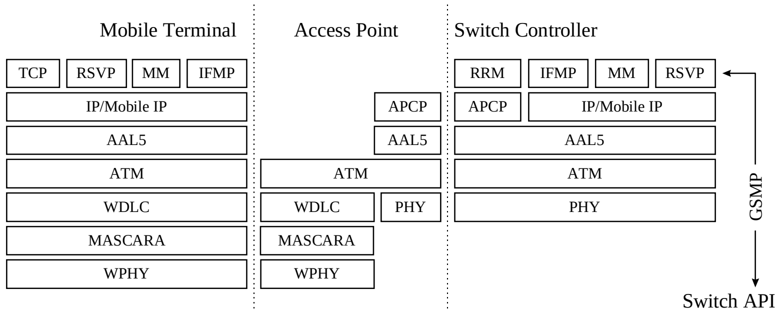

Figure 1: Architecture of a wireless broadband IP system

In the MT, the IP protocol stack is placed on top of AAL5. On top of IP, we run TCP, RSVP, IFMP and Mobility Management (MM). The Mobility Management entity is a descendant of the MMC entities found in the WAND pilot. This entity co-operates with Mobile IP and handles power-on, initial registration and handovers. However, some handover cases are handled at the radio subsystem level (see Section 4). The stack in the APs includes AAL5 as a means for exchanging control messages (e.g. wireless MAC information and statistics) with the Radio Resource Manager (RRM) of the Mobile IP router (this protocol is also referred to as APCP - AP Control Protocol). The SC stack is also AAL5-based. On top of this layer we have IP (with routing - packet forwarding capabilities), and on top of IP the Mobility Management, RSVP and IFMP entities. It is also assumed that the IP layer integrates the Mobile IP functionality, thus, acting as a Home Agent (HA) for MTs registered in the particular wireless subnet (formed by the Mobile IP router and the APs it controls).

To expedite the operation of the above mentioned protocols, apart from the QoS and BE VCs, three additional dedicated control channels are established in the MT-SC link. Such channels are intended for IFMP, MM and RSVP messages. As proposed in [Bas97], RSVP messages within the backbone network should follow the hop-by-hop routed path to allow prompt reactions to routing changes. Figure 2 illustrates the proposed architecture.

3. Mobility Requirements

The primary objective of the IP-oriented redesign of the WAND architecture is the continuous - uninterrupted provision of IP services to MTs. As the specification of Mobile-IP suggests that it is well suited for ‘macro’ mobility management, the proposed design incorporates mechanisms for the support of mobility in both the ‘macro’ and the ‘micro’ level. In the context of an IP network, the MT should retain an originally assigned address so that it is always addressable by other terminals. New addresses (care-of-addresses or *coa*) are assigned to the MT as soon as it enters the area controlled by another Mobile IP router. Handovers between APs attached to the same Mobile IP router should not result in changes propagating beyond the Mobile IP router (low-level VC diversions keep other layers unaffected). The new design aims to implement optimised handover schemes with minimum losses to protect against high delays or substantial QoS degradation. Finally, handovers should be executed rapidly and enable QoS re-negotiation. Owing to the adoption of Mobile IPv6, the datapaths leading to MTs are optimal and triangular routing is avoided.

4. Mobility across the WAND Access Network

Three handover types are envisaged for the WAND architecture:

- intra-AP,
- intra-subnet, and
- inter-subnet handovers.

The intra-AP handover is a radio handover, i.e., the MT switches to another frequency in the same AP; the handover is handled exclusively by the AP without additional signalling or the involvement of higher level entities. The intra-subnet handover refers to the case where the MT moves between different APs, which are controlled by the same mobile IP-router. Finally, the inter-subnet handover deals with the mobility of the MT between APs that are controlled by different mobile IP-routers. A brief overview of the last two handover schemes - which involve signalling entities - is provided below.

4.1 Intra-subnet Mobility

When the MT roams within the control area of an Mobile IP router (intra-AP and intra-subnet handovers), it remains within the same IP subnet, and thus retains its assigned IP address. In the case of intra-subnet handover, CAC (Connection Admission Control) has to the be performed for the new target AP. There are two CAC functions, one for the fixed network (Fixed CAC refers to resources in the switch - AP link), and one for the wireless part (Wireless CAC refers to radio resources). Fixed CAC is handled by RSVP's traffic control entities, while the Wireless CAC is performed in the SC on the basis of information provided by the AP through the APCP (Figure 1). The QoS characteristics of each active connection are maintained within the SC (Flow table). If CAC algorithms grant admission, VCs pertaining to the moving MT are diverted to the new link. GSMP is used for this interaction between the SC and the IP switch. If the new AP can support lower QoS than requested, the MT has the option of

- accepting the modified QoS offered by the network,
- converting the connections to best-effort, or
- completely dropping the connections.

In such cases, RSVP messages indicating modifications or cancellations of the reservations are propagated to the correspondent node so as to notify it on the changes regarding the connections' requirements. Resources allocated to the connections in the old/source AP are released through the use of explicit RSVP signalling (instead of leaving reservations time-out). The primary goal during the execution of a handover is to preserve the control channels (RSVP, MM and IFMP VCs) in the new AP. Since the handover is confined within the same switch, no Mobile-IP specific signalling is exchanged. Figure 3 shows the interfaces needed between the MM and other SC entities for the realisation of handovers.

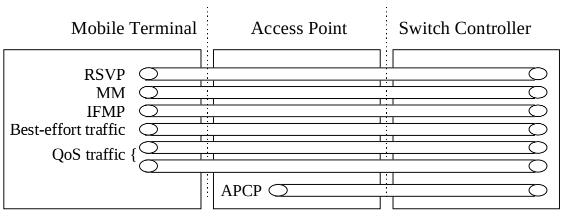

Figure 2: Allocated VCs in the MT-SC link

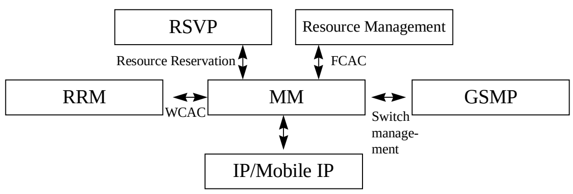

Figure 3: Interfaces of MM module

4.2 Intra-subnet Handover Optimisations

The proposed intra-subnet handover scheme is prone to data loss and delays. We examine some techniques to overcome such problems. The main obstacle in eliminating data loss is the lack of identification for the ATM cell headers. In case of duplication, loss or misordering of cells, the reconstructed IP datagram will be considered corrupted in the AAL5 layer. One approach suggests the insertion of marker cells in the data flows (as a means of inband signalling) [Mit96]. Marker cells co-ordinate the sequence of the ATM cells to be transmitted by the target/new AP. In the case of handover, part of the cell stream has to be relocated to the target/new AP. This scheme facilitates data loss prevention. An enhancement to this solution, which also capitalises on the IP-orientation of the proposed architecture, would be multicasting towards previous and potential target/new APs. The AP to which the MT is currently attached transmits the cells over the radio interface, while the potential target/new APs buffer them for future use. A similar approach, on the datagram level, has been adopted in the Daedalus project [Sri96] implemented in the University of California at Berkeley (UCB).

4.3 Inter-subnet mobility

When an MT moves to an AP connected to a different switch than that of the previous AP, an inter-subnet HO is performed. During the progress of handover, the previous coa remains valid, thus giving the chance to the MT to receive datagrams from the old AP (previous switch) by a simple forwarding mechanism based on IP-in-IP encapsulation. A new coa is obtained by the MT in the new subnet, additionally to the establishment of control channels (IFMP, RSVP, MM). Address allocation is performed by the Stateless Address Autoconfiguration mechanism [Tho96], which is based on a reserved link-local subnet address and the interface identifier. Using this temporary address, the MT can either obtain a local subnet address using the Neighbour Discovery [Nar96] protocol (actually, router solicitation and advertisements are used) or it can contact a DHCP server (or a relay, since the DHCP server must reside on the same subnet due to the link local communication) to obtain an administered address. The newly acquired coa is registered with the MT's Home Agent by means of the Binding Update and Binding Update Acknowledgement messages. The MT also sends Binding Update messages to each CN and the previous router. Thus, any packet received by the previous router will now be forwarded to the new sub-net. This is aligned with the effort to keep the handover lossless. However, the QoS guarantees are not preserved during handover as shown in the Message Sequence Chart (MSC) in Figure 4. The reservation of resources in the new path will not be effected immediately, causing QoS traffic to be temporarily exchanged over the BE channel.

If QoS connections exist from the CN to the MT, the former will issue PATH messages upon reception of the Binding Update message. The Binding Update message is a prerequisite for the transmission of PATH messages by the CN, as its Binding Cache has to be updated in accordance to MT's change of coa. The MT will respond with RESV messages. If QoS connections exist in the opposite direction, the MT issues, upon reception of Binding Update Acknowledgement, RSVP PATH messages towards the CN for updating/installing state information in the intermediate routers. The CN will react with RESV messages. Similarly to the intra-subnet HO case, the same CAC procedure for the wireless link in the new subnet and on the new router is performed. Fixed CAC is triggered by RSVP. After the completion of the above activities, the CN should issue RESVTEAR messages in the route towards the previous router. The RSVP entity within the router should start releasing resources in the reverse direction (flows having the MT acting as Sender). The two re-establishments (MT to CN, CN to MT) can be overlapped and not necessarily executed sequentially as show in Figure 4.

Two important reasons support the above solution. First, the forwarding mechanism guarantees that all packets arrive at the new location of the MT. The drawback here is a temporary increase in delay. However, this is mostly dependent on the IP-in-IP encapsulation performance of mobile IP routers, and can be optimised in this respect. Secondly, the period of BE transmission of data towards the mobile is very short if the above described interaction between Mobile IP and RSVP is implemented. Binding updates (and the associated acknowledgements) trigger the regeneration of PATH messages if there are reserved flows. This interaction requires only a small interface added to the RSVP demons and it guarantees the flow to recover its QoS requirements after at least 1.5 round-trip delays between CN and MT.

In this approach (forwarding combined with PATH message triggering), another problem should be investigated: what happens in a saturated backbone link where our MT has just been granted a reservation and must release it for a few milliseconds until the new path state is setup? Chances are that somebody else will get the bandwidth (since there is congestion) once the reservation is torn down or it expires. How can we ensure that the bandwidth (or other reserved resource) is handed over to the new flow? Sending the old RESVTEAR and new RESV message together; nevertheless, the behaviour of admission control in routers is still implementation dependent. What would be needed is a RESVEXCH (RESerVation EXCHange) message that does a TEAR and RESV in an atomic operation. However, this would be no longer an unchanged protocol, which was one of our goals. A more sensible solution to the problem is to delay the de-allocation of resources on a RESVTEAR message (i.e., extend the soft-state behaviour) and wait for a potential new RESV message that differs only in the sub-net part of the MT address and has same CN addresses and same last part of the MT address (MAC address of MT according to the address allocation mechanism described above). Of course, such an approach complicates processing of RESV messages, but its advantages are an unchanged RSVP and transparent 'handover' of reserved resources.

To expedite the above described scenario, the new router could be informed about the RSVP state information from the previous router. RSVP, however, uses Destination Address (DestAddress) as part of the session identification information. Since the destination address changes (connections towards the MT), new RSVP sessions need to be established. In [Tal97], an extension to the RSVP protocol is proposed called MRSVP. MRSVP introduces RSVP proxy agents in routers. Proxy agents communicate with each other and reserve the resources for future use by MTs. Reservations are distinguished in “active” and “passive”. An active reservation corresponds to a flow over which data is actually exchanged. A passive reservation on the other hand corresponds to a flow in which the resources are reserved along the route, but data is not passing through. This leads to poor network utilisation, since reserved resources are not used. A modification of the inter-subnet handover based on the proposed scheme is illustrated in Figure 5.

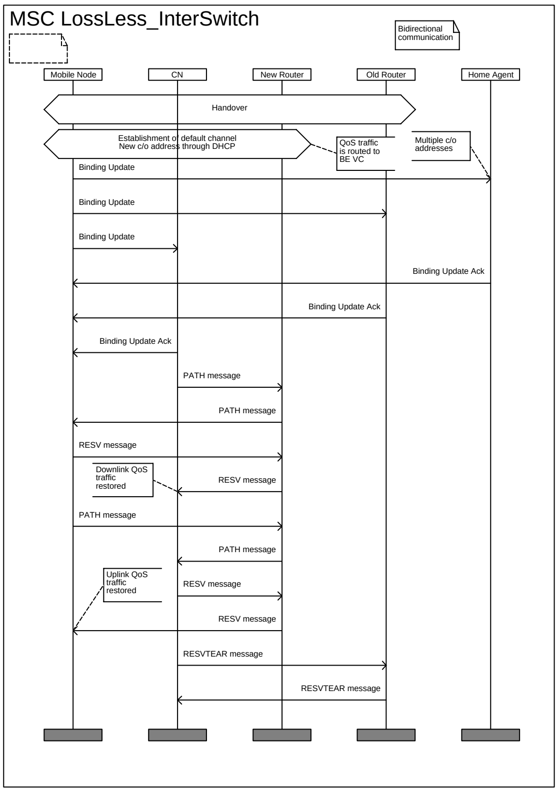

Figure 4: Inter-subnet HO

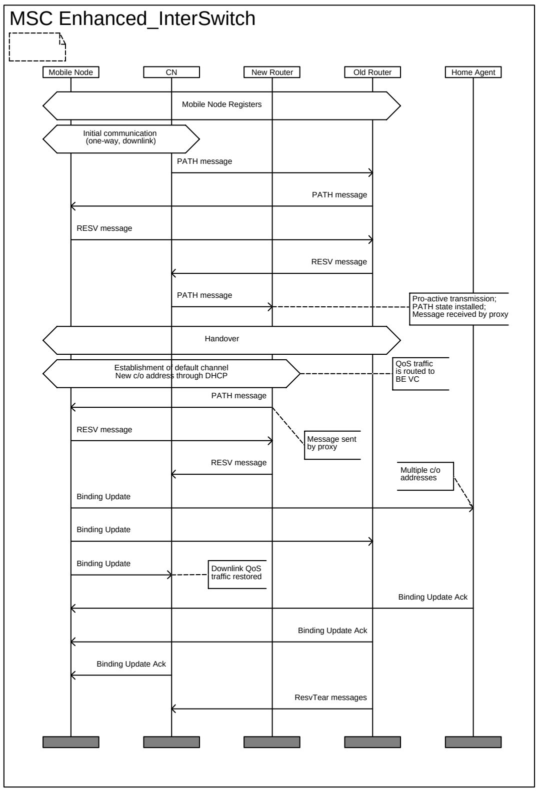

Figure 5: Enhanced inter-subnet HO

In WAND, we are investigating the possibility of having the path state information in the new router prior to the execution of a handover. This could be accomplished by forcing the CN to send (pro-actively) PATH messages to coas residing in subnets which are expected to be visited by the MT after handover. Having the path state information already in place, it would only require a RESV message from the MT to re-establish the QoS connection. The RESV message would also probably not propagate too much in the network between the router and the CN, because it is a side-effect of a handover procedure (i.e., it is highly probable that the two routers are located close to each other and are probably connected to a nearby router). Apart from the technical difficulties that this solution imposes, it also leads to unacceptable waste in network resources due to its pro-active orientation. Technically, the solution requires the CN to be capable of sending PATH messages to more than one coas. This is troublesome, though, due to the specification of MT's Binding Update Cache and RSVP's placement on top of Mobile IP. Serious modifications to the binding cache will be needed for making the mechanism transparent to other layers.

An alternative, but quite similar, approach would be the extension of RSVP sessions from the current router towards the new. This communication does not involve Path message transmissions from the CN. Additionally, the old RSVP sessions need not be terminated. In the target router, resources would have been a-priori reserved according to the proxy-based scheme. This technique, also known as "Path Extension" [Ach97], may result in sub-optimal paths if the MT executes consecutive inter-subnet handovers.

5. Conclusions

In this paper, we have discussed the WATM architecture tuned for IP that the WAND consortium is currently studying in the context of the project's extension activities. We have presented the targeted architecture and protocol stacks, and considered mobility management issues. The introduction of RSVP for IP connections with QoS requirements entails substantial difficulties in the realisation of inter-subnet handovers. QoS connections are temporarily constrained to the best-effort service class due to the required re-establishment of RSVP sessions. Although, with minor modifications to the behaviour of these protocols, the system can be reasonably designed, a perfect solution is unlikely to be achieved without changes to Mobile IP or RSVP.

References

[Ach97] A. Acharya, J.Lin, B. Rajagopalan and D. Raychaydhuri, *Mobility Management in Wireless ATM Networks*, IEEE Communications Magazine, Vol.35, No.11, pp.100-109, November 1997.

[Ala98] J. Ala-Laurila, J. Seppälä, L. Stacey and N. Nikaein, *Designing a Wireless Broadband IP Access System with QoS Guarantees,* to be presented in the ACTS Mobile Summit '98, Rhodes, Greece.

[Bas97] E. Basturk, A. Birman, G. Delp, R. Guerin, R. Haas, S. Kamat, D. Kandlur, P. Pan, D. Pendarakis, R. Rajan, D. Saha and D. Williams, *Design and Implementation of a QoS Capable Switch-Router*, IBM Research Report, RC 20848 (01/31/97).

[Bra97] R. Braden, L. Zhang, S. Berson, S. Herzog and S. Jamin, *Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification*, RFC 2205, IETF Network Working Group, September 1997.

[Dee95] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC 1883, Network Working Group, December 1995.

[Joh97] D. Johnson and C. Perkins, *Mobility Support in IPv6*, Internet Draft (draft-ietf-mobileip-ipv6-04), Mobile IP Working Group, November 1997.

[Kal96] A. Kaloxylos, S. Hadjiefthymiades and T. Kuehnel, *Req. Specification of Mobility Management and Control*, The Magic WAND, Deliverable 4D4, ACTS Programme, December 1996.

[Mit96] H. Mitts, H. Hansén, J. Immonen and S. Veikkolainen, *Lossless handover for wireless ATM,* Proceedings of ACM MobiCom, NY, USA, November 1996.

[Nar96] T. Narten, E. Nordmark, W. Simpson, *Neighbor Discovery for IP Version 6*, RFC 1970, August 1996.

[New96] P.Newman et al, *Ipsilon's General Switch Management Protocol Specification - Version 1.1*, RFC 1987, Network Working Group, August 1996.

[New97] P. Newman, G. Minshall, T. Lyon and L. Huston, *IP switching and Gigabit Routers*, IEEE Communications Magazine, January 1997.

[Sri96] S. Srinivasan, H. Balakrishnan and R. Katz, *Handoffs in Cellular Wireless Networks, The Daedalus Implementation and Experience*, Kluwer International Journal on Wireless Comm. Systems, 1996.

[Tal97] A.K. Talukdar, B.R. Badrinath and A. Acharya, *MRSVP: A reservation protocol for an Integrated Services Packet Networks with Mobile hosts*, Technical report, DCS-TR-337, Rutgers University, 1997.

[Tho96] S. Thomson and T. Narten, *IPv6 Stateless Address Autoconfiguration*, RFC 1971, Network Working Group, August 1996.