Unified QoS Provision in Wireless Access Networks

Nikos Passas and Lazaros Merakos
Dept. of Informatics & Telecommunications
University of Athens
Athens, Greece
{passas,merakos}@di.uoa.gr

***Abstract*—A scheme that uses the Inter Access Point Protocol (IAPP), currently standardized by IEEE, for path re-establishments after handover is proposed. According to this scheme, the Access Point that a Mobile Node moves to, can act as a proxy for the required RSVP signaling. The scheme is applicable to all IP-based wireless access systems, and can work in conjunction with the standard RSVP protocol, as well as partial re-establishment methods. The paper also includes a detailed description of the structure of the required messages. Besides reducing handover latency and signaling overhead, the proposed scheme also allows for the operation of advanced admission control algorithms in the new Access Point.**

Keywords: RSVP, Wireless LANs, IAPP, handover

I. Introduction

Next Generation Networks (NGNs) are expected to integrate a large number of access networks in one IP-based core. One of the most important problems towards this direction is the Quality of Service (QoS) provision. To treat the problem of QoS in IP networks, the Internet Engineering Task Force (IETF) has introduced two main frameworks, namely the Integrated Services (IntServ) [1] and the Differentiated Services (DiffServ) [2]. DiffServ classifies and possibly conditions the traffic, in order to ensure similar behavior throughout the network. It performs well in core networks, due to its scalability to support large numbers of flows. IntServ on the other hand, is targeted mainly for the access systems, by providing means to request and obtain end-to-end QoS per flow. The Resource Reservation Protocol (RSVP) [3] is considered the most popular signaling protocol in IntServ for requesting QoS per flow, and setting up reservations end-to-end upon admission.

Additionally, the growing demand of users for mobility support has led to the considerable development of a large number of heterogeneous access networks. Especially wireless local area networks (WLANs), offering indoor and limited outdoor communications, are becoming more and more popular and tend to replace the traditional wired LANs. Designated exclusively for access systems, WLANs have to incorporate IntServ to be compatible with the QoS schemes followed in fixed access systems. The use of RSVP is problematic in wireless access networks mainly due to the unstable wireless links, which lead to variable available bandwidth, and, the need for mobility, which results in changes of the established paths.

In this paper, we discuss the problems of RSVP in mobile nodes, and propose a unified scheme for WLANs that aims at reducing path re-establishment delays. The rest of the paper is organized as follows. Section II briefly presents the operation of RSVP, and how it is influenced during handovers. Section III describes in detail the proposed scheme. In Section IV, the required RSVP objects that should be transmitted are depicted. Finally, Section V presents our conclusions.

II. RSVP and Mobility

RSVP is used in the IntServ framework for requesting QoS per flow and setting up reservations upon admission. More specifically, it defines a communication *"session"* as a data flow with a particular destination and transport layer protocol, identified by the triplet (destination address, transport-layer protocol type, destination port number). Its operation only applies to packets of a particular session, and therefore every RSVP message must include details of the session to which it applies. The two most important messages of the RSVP protocol are the PATH and RESV messages. The PATH message is initiated by the sender and travels towards the receiver to provide characteristics of the anticipated traffic, as well as measurements for the end-to-end path properties. The RESV message is initiated by the receiver, upon reception of the PATH message, and carries reservation requests to the routers along the communication path between the receiver and the sender. After the path establishment, PATH and RESV messages should be issued periodically to maintain the so-called *"soft states"* that describe the reservations along the path.

Designed for fixed networks, RSVP assumes fixed end-points and for that reason its performance is problematic in mobile networks. When an active mobile node (MN) changes its point of attachment with the network (e.g., in handover), it has to re-establish reservations with all its corresponding nodes (CNs) along the new paths. For an outgoing session, the MN has to issue a PATH message immediately after the routing change, and wait for the corresponding RESV message, before starting data transmission through the new attachment point. Depending on the hops between the sender and the receiver, this can cause considerable delays, resulting in temporary service disruption. The effects of handover are even more annoying in an incoming session because the MN has no power for invoking immediately the path re-establishment procedure. Instead, it has to wait for a new PATH message, issued by the sender, before responding with a RESV message in order to complete the path re-establishment. Simply decreasing the period of the soft state timers is not an efficient solution, because this could increase signaling overhead significantly.

A number of proposals can be found in the literature for reducing the effects of RSVP path re-establishment during handover, but many of them require considerable enhancements or alterations of the protocol operation. In micro-mobility environments, only a small part of the path is changed, while the remaining circuit can be re-used. Accordingly, a scheme for partial path re-establishment can be considered, which handles discovery and setup of the new part between the crossover router and the MN. The number of hops required to set up the partial path during a handover depends on the position of the crossover router. Such a scheme can reduce resource reservation delays, and provide better performance for real-time services, without affecting the operation of RSVP considerably.

In the next section, a scheme is proposed that can be used either with the original RSVP protocol, or in conjunction with proposals for partial path re-establishment like [4] and [5]. It aims at further reducing the path re-establishment time, through the use of IAPP. According to the proposed scheme, RSVP context information for the active sessions of the MN is transferred from the old to the new Access Point (AP), in order to allow it to act as a proxy of the MN for the required RSVP signaling. In this way, the new AP is able to initiate the required (full or partial) path re-establishment for all active sessions of the MN, accelerating the whole process. This prevents the MN from waiting to perform RSVP signaling for each one of the active sessions after re-association with the new AP.

III. RSVP AND IAPP

The Inter Access Point Protocol (IAPP) is a recommended practice currently standardized by the IEEE Working Group 802.11f, that provides the necessary capabilities for transferring context from one AP to another, through the fixed distribution system, in order to facilitate fast handovers across multi-vendor APs (Figure 1). Although initially proposed for 802.11 networks, it can be used to any kind of WLANs with a TCP/IP distribution system. The current draft [6] describes a service access point (SAP), service primitives, a set of functions and a protocol that will allow conformant APs to interoperate on a common distribution system, using the Transmission Control Protocol over IP (TCP/IP) to exchange IAPP packets.

The IAPP message exchange during handover is initiated by the *re-associate* message, which carries the Basic Service Set Identifier (BSSID) of the old AP (message 1 in Figure 1). In order to communicate with the old AP through the fixed distribution system, the new AP needs its IP address. The mappings between BSSIDs and IP addresses can be either stored inside all APs or obtained from a Remote Authentication Dial-In User Service (RADIUS) server (messages 2 and 3). If communication between APs needs to be encrypted, security blocks are exchanged before actual communication (messages 4 and 5). The two most significant messages of the IAPP are the *MOVE-notify* (message 6), issued by the new AP to inform the old AP that the MN has moved to its area, and the *MOVE-response* (message 7), issued by the old AP, containing the *Context Block*. The MOVE-notify and MOVE-response are IP packets carried in a TCP session between the two APs. Although initially intended to contain authentication information, to allow the new AP to accept the MN without re-authentication, the Context Block has a flexible structure, able to support any information exchange. More specifically, it can consist of a variable number of *Information Elements* (IEs) of the form (Element ID, Length, Information). In this way, every IE can contain variable length information, whose type is specified by the Element ID. Processing of the information transferred inside the IEs is beyond the scope of the IAPP, and depends on the functionality of the APs. Recently, a caching mechanism has been added in IAPP that aims at facilitating handovers by proactively sending context information to neighboring APs. According to this mechanism, in a handover the new AP should first lookup into its cache for the MN's Context Block. If not found, then a MOVE-notify message is issued towards the old AP.

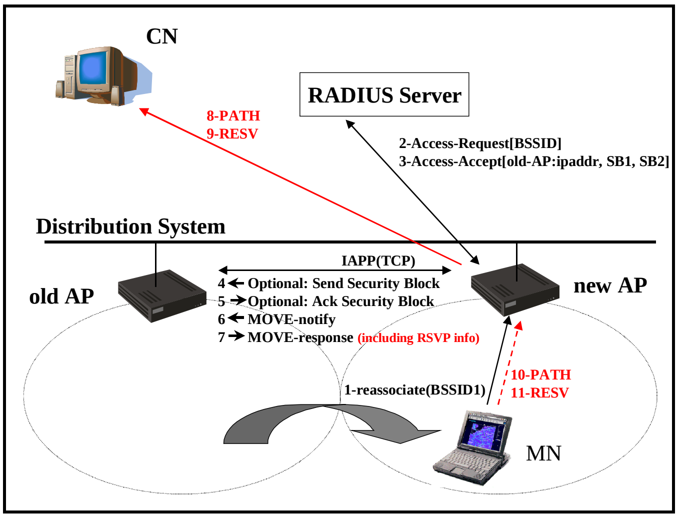

Figure 1. The IAPP/RSVP operation

According to [6], the Context Block may include IEs with the required authentication information, in order to allow the new AP to accept the MN without re-authenticating it and reduce the handover delay. In the scheme proposed here, the flexible Context Block structure can also include IEs carrying RSVP information, in order to accelerate the required path re-establishment process through the new AP, and further reduce handover latency. The structure of IEs required for RSVP information is described in detail in the next sections. In brief, one IE is used per active outgoing or incoming session, containing the details required for the new AP to create the corresponding PATH or RESV state respectively. The aim is to allow the new AP to act as a proxy for initiating RSVP messages towards the network on behalf of the MN, before the completion of the re-association process. As shown below, the IE should contain the session identification triplet (destination address, transport-protocol type, destination port) and the traffic descriptor (SENDER_TEMPLATE and SENDER_TSPEC) objects of RSVP. Similarly, for an incoming session, the IE should contain the session identification, the flow descriptor (FLOWSPEC and FILTER_SPEC) and the reservation style (STYLE) objects.

Since the new AP might be more crowded than the old one, or can provide lower available bandwidth, some of the sessions might not be possible to be supported. Consequently, an admission control algorithm should be applied in the new AP to decide on which sessions can be accepted, based on the RSVP information received through the MOVE-response message. For an accepted outgoing session, the new AP immediately creates the respective PATH state and issues a PATH message towards the network (message 8), without waiting to receive this message from the MN after the re-association process is finished. For denied outgoing sessions, the new AP can either omit the PATH messages, and let reservations expire, or send PATH_Tear messages to release resources along the paths. Concerning an active incoming session, as soon as the new AP receives the PATH message from the network, it immediately creates a RESV state and responds back with the respective RESV message (message 9), without waiting for the MN to issue it, provided the specific session was accepted during admission control. In different case, the PATH message is either ignored, or a RESV_Tear message is issued to release the resources along the path.

According to the above procedure, the new AP does not have to wait for the MN to send the required RSVP messages after re-association. Additionally, assuming the MN is aware of the IAPP usage to transfer the RSVP context to the new AP, it can omit sending the PATH and RESV messages (messages 10 and 11 respectively) for the active sessions and just wait for the paths re-establishment. In this case, for an outgoing session the MN can start transmitting data as soon as it receives the RESV message from the new AP, while for an incoming session, the MN can simply wait to receive data packets. In this way, signaling overhead and re-establishment delays are reduced during handover.

Figures 2 and 3 present an example of standard and proposed signaling sequence for an outgoing session respectively. In Figure 2, the IAPP is used to transfer only authentication information, while in Figure 3 it transfers RSVP information as well. The proposed scheme can also work together with a partial path re-establishment solution like [4] and [5]. The only change is that the new AP communicates with the crossover router instead of the CN. A side effect of the proposed scheme is that it transmits the full set of RSVP traffic and QoS information for active sessions to the new AP inside a single message (MOVE-response). This allows for advanced admission control algorithms in the new AP, in order to decide on which sessions can be accepted in case bandwidth is insufficient. This is not possible in the regular case, where path re-establishment requests arrive sporadically from the MN after re-association.

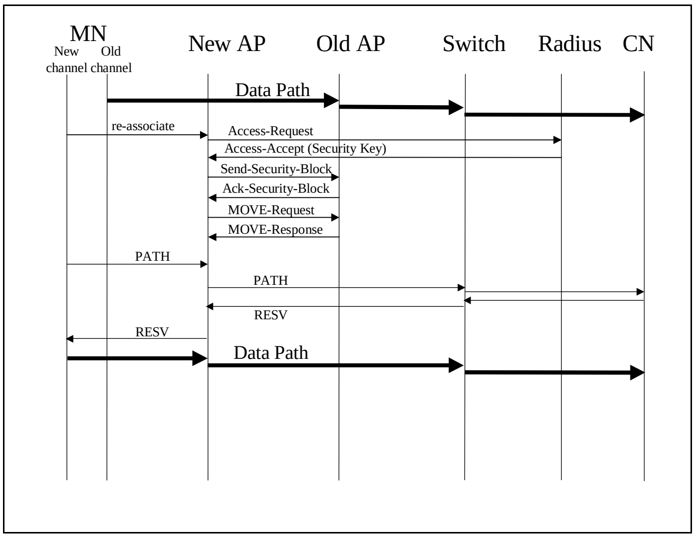

Figure 2. Standard message exchange for outgoing sessions

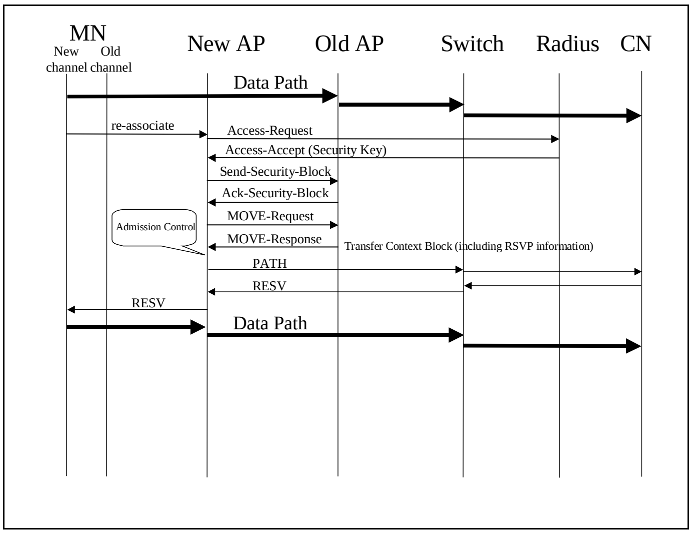

Figure 3. IAPP-assisted RSVP message exchange for outgoing sessions

IV. RSVP Information Elements Structure

PATH and RESV messages contain a large set of objects, in order to cover all network cases. For example, they contain objects to indicate non-RSVP nodes, or nodes without policy control, objects for authentication or confirmation. Most of these objects can be omitted from the respective IAPP information elements. More specifically, the PATH IE should contain the objects that describe the traffic that the sender intends to enter to the network, i.e., the SESSION, SENDER_TEMPLATE and SENDER_TSPEC objects, while the RESV IE should contain the objects describing the anticipated offered bandwidth and QoS, i.e., the SESSION, STYLE and flow descriptor list (consisting of FLOWSPEC and FILTER_SPEC objects).

According to [3], each object consists of one or more 32-bit words with a one-word header, with the following format:

```
        0             1              2             3
+-------------+-------------+-------------+-------------+
|       Length (bytes)      |  Class-Num  |   C-Type    |
+-------------+-------------+-------------+-------------+
|                                                       |
//                  (Object contents)                  //
|                                                       |
+-------------+-------------+-------------+-------------+
```

Length is a 16-bit field containing the total object length in bytes, *Class-Num* identifies the object class, while *C-Type* is unique within Class-Num and at the moment can take two values indicating IPv4 or IPv6 addressing.

In Figures 4 and 5, an example for the structure of the PATH and RESV IEs is given respectively. We assume IPv4 addressing, Fixed-Filter style and Guaranteed Service. For IPv6, the only difference is that source and destination addresses occupy 16 bytes instead of 4. Guaranteed Service is considered for the FLOWSPEC, in order to offer bounded end-to-end delays and bandwidth. For Controlled-Load Service the FLOWSPEC should not include the *Rate* and *Slack Term* parameters. Details for the specific fields can be found in [3] and [7].

It is clear that many fields inside the objects could be omitted or forced to consume less space. Nevertheless, the objects are included as defined for RSVP in order to be compatible with future versions of the RSVP protocol that use more fields. Additionally, the above IE structure is flexible in including more objects if needed. The only thing that is needed in order to include a new object is to add the object at the end of the respective IE, as defined in RSVP together with its object header, and update the IE Length field accordingly. In the example presented above, the length of the PATH IE is 64 bytes, while the length of the RESV IE is 84 bytes. Note that using the IAPP, this information is transmitted through a high-speed distribution system connecting the two APs. In different case, the same information would have to be transmitted using standard RSVP signaling through the wireless medium, after re-association of the MN with the new AP, resulting in considerable delays and signaling overhead.

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+........-+-+
|      IE ID = PATH IE          |            IE Length           |  Value |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+........-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=8        | Class-Num=1   |  C-Type=1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               IPv4  DestAddress                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Protocol Id   |     Flags     |             DstPort           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=8        | Class-Num=11  |  C-Type=1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               IPv4 SrcAddress                                 |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    //////     |    //////     |             SrcPort           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=32       | Class-Num=12  |  C-Type=2     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0 (a) |    reserved           |               7 (b)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    1  (c)     |0| reserved    |               6 (d)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   127 (e)     |     0 (f)     |               5 (g)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Token Bucket Rate [r] (32-bit IEEE floating point number)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Token Bucket Size [b] (32-bit IEEE floating point number)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Peak Data Rate [p] (32-bit IEEE floating point number)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Minimum Policed Unit [m] (32-bit integer)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Maximum Packet Size [M]  (32-bit integer)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4. An example of PATH IE structure

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+........-+-+
|      IE ID = RESV IE          |             Length             |  Value |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+........-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=8        | Class-Num=1   |  C-Type=1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               IPv4  DestAddress                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Protocol Id   |     Flags     |             DstPort           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=4        | Class-Num=8   |  C-Type=1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Flags        |            Option Vector                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=8        | Class-Num=10  |  C-Type=1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                     IPv4 SrcAddress                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    //////     |    //////     |             SrcPort           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|       Length (bytes)=8        | Class-Num=9   |  C-Type=2     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| 0 (a) |    Unused             |              10 (b)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    2  (c)     |0| reserved    |               9 (d)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   127 (e)     |     0 (f)     |               5 (g)           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Token Bucket Rate [r] (32-bit IEEE floating point number)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Token Bucket Size [b] (32-bit IEEE floating point number)    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Peak Data Rate [p] (32-bit IEEE floating point number)       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Minimum Policed Unit [m] (32-bit integer)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Maximum Packet Size [M]  (32-bit integer)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     130 (h)   |     0 (i)     |              2 (j)            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Rate [R]  (32-bit IEEE floating point number)                |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Slack Term [S]  (32-bit integer)                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 5. An example of RESV IE structure

V. Conclusions

A unified scheme, which uses the IAPP in order to facilitate RSVP path re-establishments after handover in heterogeneous wireless access networks, was proposed. The scheme is applicable to all kinds of IP-based wireless access systems. By transferring the required RSVP information through proper IAPP Information Elements, the scheme allows the new AP to act as a proxy of the MN for the required RSVP signaling, and start the path re-establishment process before the end of re-association. In this way, both handover latency and signaling overhead in the wireless medium are reduced. Additionally, the full set of traffic and QoS information for all active sessions is transferred to the new AP through a single message, allowing for efficient admission control.

Future plans include the introduction of an efficient admission control algorithm for the new AP, in order to decide on which sessions can be accepted in cases where the available bandwidth in the new cell is insufficient to support the full set of active MN sessions. The decision should be based on several factors, such as session priority, traffic and QoS requirements, and bandwidth utilization.

Acknowledgments

This work has been produced in the framework of the project "ANWIRE" (IST-2002-38835), which is funded by the European Community. The authors would like to acknowledge the contributions of their colleagues from University of Athens, King's College London, University of Helsinki, Rheinisch-Westfaelische Technische Hochschule Aachen, Universita Degli Studi di Catania, Universidad Politécnnica de Madrid, Instituto Superior Técnico, Universite Pierre et Marie Curie, University of Cyprus, University of Limerick, Ecole Nationale Supérieure des Télécommunications, NEC Europe Ltd, Thales Communications, Thales Research Limited, University of Surrey, Centre Tecnològic de Telecomunicacions de Catalunya.

References

[1] R. Braden et al., "Integrated Services in the Internet Architecture: an Overview," *RFC 1633*, June 1994.

[2] DiffServ

[3] R. Braden et al., "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification," *RFC2205*, September 1997.

[4] S. Paskalis et al., "An Efficient RSVP/Mobile IP Interworking Scheme," *ACM Mobile Networks Journal*, vol. 8, no. 3, June 2003.

[5] B. Moon and A. H. Aghvami, "Reliable RSVP Path Reservation for Multimedia Communications under IP Micro Mobility Scenario," *IEEE Wireless Communications Magazine*, October 2002.

[6] IEEE Std. 802.11f/Draft 5, "Draft Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation," available at *http://www.cs.umd.edu/~mhshin/doc/802.11/802.11F-D5.pdf*, January 2003.

[7] J. Wroclawski et al., "The Use of RSVP with IETF Integrated Services", *RFC2210*, September 2002.