WLAN Signaling Enhancements for Improved Handover Performance

Nikos Passas*, Apostolis Salkintzis+, Georgios Nikolaidis*, and Mary Katsamani*

*Department of Informatcis & Telecommunications
University of Athens
Panepistimiopolis, 15784, Athens, Greece
e-mail: {passas|nikolaid|grad0480}@di.uoa.gr

+Motorola
32 Kifissias Av.
15125, Athens, Greece
email: salki@motorola.com

Abstract— **This paper focuses on the performance evaluation of a novel scheme that extends signaling in the *Inter Access Point Protocol* (IAPP), in order to expedite the RSVP path re-establishment that takes place after a handover from one WLAN Access Point (AP) to another, and reduce data blocking time. The prime characteristic of this scheme is that the mobile node returns back to the old AP during signaling exchange in the fixed network, in order to maintain connectivity. Additionally, the new AP serves as an RSVP proxy that starts signaling on behalf of the mobile node much earlier compared to the standard RSVP operation in a WLAN. Therefore, a considerable handover latency reduction can be achieved, especially under heavy traffic conditions. To evaluate the performance and the benefits of the proposed scheme, we display and discuss a series of simulation results.**

Keywords— **IAPP, RSVP, handover, path re-establishment.**

I. INTRODUCTION

The demand for multimedia services in mobile networks has raised several technical challenges, such as the minimization of handover latency. In this context, soft and softer handover techniques have played a key role and provided the means for eliminating the handover overhead and thus enabling the provision of mobile multimedia services. However, not all radio access networks support soft handover techniques. For example, the notorious IEEE 802.11 WLANs support only hard handovers and consequently the support of multimedia services over such WLANs raises considerable concerns. Recently, a lot of effort has been placed on addressing these concerns and a notable example is the development of the Inter Access Point Protocol (IAPP) [1] by IEEE 802.11 Task Group f, which provides standardized means for transferring *context* from one Access Point (AP) to another, through a fixed distribution system, in order to reduce handover latency.

Another major challenge in both fixed and wireless networks today is Quality of Service (QoS) provision. For wireless access networks, such as WLANs, the Integrated Services (IntServ) framework [2], standardized by the Internet Engineering Task Force (IETF), provides the necessary means for requesting and obtaining QoS per flow. IntServ uses the Resource ReserVation Protocol (RSVP) [3] for implementing the QoS signaling. As discussed in the next section, RSVP is problematic in wireless networks, basically due to the need for re-establishing resource reservations every time a Mobile Node (MN) moves to a new subnet and the IP route with its Corresponding Node (CN) changes.

This paper provides an extension to the proposal made in [4], that aims at further reducing the data blocking time during handover. In that proposal, IAPP is used for transferring between two APs (from old AP to new AP) the RSVP context that pertains to a particular MN. Using this context, the new AP can initiate the RSVP signaling required for re-establishing the reservation paths of active MN flows, in order to reduce the handover latency. Here, we extend this idea by introducing enhancements to IAPP, referred to as IAPP+ that allow the MN to move back to the old AP, during the required message exchange in the fixed network, in order to reduce data blocking time, and improve QoS in handover.

The rest of this paper is organized as follows. Section II discusses the operation of IAPP for transferring context information between APs. Section III presents the proposed IAPP+ scheme. Section IV describes the contents and structure of the RSVP context information that needs to be transferred through IAPP for every outgoing or incoming flow. Section V contains the description of the simulation model constructed for evaluating the proposed scheme, and the obtained numerical results. Finally, section VI presents the conclusions and plans for future work.

II. THE OPERATION OF IAPP

IAPP is a recommended practice recently 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. The operation of the protocol is depicted in Figure 1. The standard [1] 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 [5] (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 own area, and the *MOVE-response* (message 7), issued by the old AP, containing a *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 type of 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.

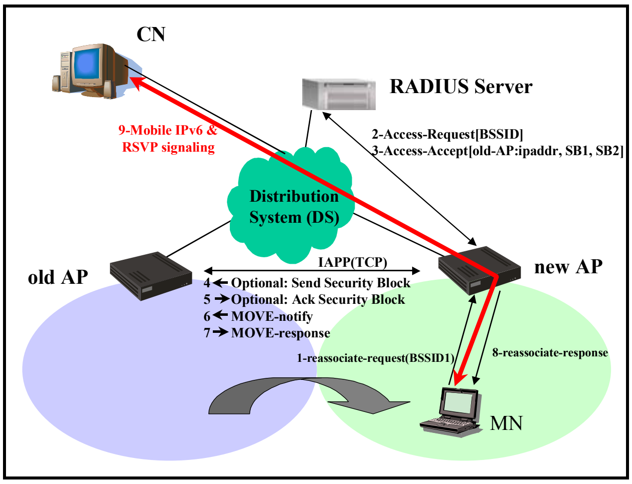


Figure 1. Standard IAPP and RSVP signaling

III. The Proposed Scheme

During handover of a Mobile Node (MN) from one AP (old AP) to another (new AP), the aim of the IAPP is to avoid time-consuming procedures that in different case would be needed before transmitting through the new link. The two most significant messages of IAPP are the *MOVE-Request*, issued by the new AP to inform the old AP that a MN has moved to its area, and the *MOVE-Response*, issued by the old AP, containing the Context Block (see Figure 1). Although initially intended to contain authentication information, to allow the new AP to accept the MN without re-authentication and reduce handover latency, the Context Block has a flexible structure able to transfer any kind of information.

Further to the above, the use of delay-sensitive multimedia applications mandate the WLAN to be compatible with the QoS provision framework supported by fixed IP networks. The Integrated Services (IntServ) framework is considered today the most suitable technique for the IP access networks, where WLANs are mainly targeted for. IntServ uses the RSVP signaling protocol for establishing virtual circuits, referred to as *"sessions"*, that provide per flow QoS. Although RSVP is efficient for fixed end-points, its performance deteriorates significantly for mobile nodes. When an active MN changes location (e.g., in handover), it has to re-establish reservations with all its Corresponding Nodes (CNs) along the new paths before continue transmitting, resulting in temporary disruption of service. A number of proposals can be found in the literature, trying to minimize the effects of handover in RSVP. [4] shows that the use of IAPP to transfer RSVP information during handover can significantly decrease path re-establishment delays, since it allows the new AP to act as a proxy and start the required signaling before the end of the handover process. Here, this idea is extended to combine the RSVP signaling with an enhanced version of the IAPP, in order to further reduce data blocking time and improve QoS during handover.

The key concept of the proposed IAPP+ scheme is briefly summarized below and illustrated with the aid of Figures 2 and 3. Standard IAPP and RSVP messages are marked with solid lines, while new messages are marked with dashed lines. When a MN decides to handover, it switches to the frequency of the new AP, transmits the *Reassociate-Request* message and immediately switches back to the old AP to continue data transmission. By means of conventional IAPP signaling (*MOVE-Response* message), the new AP receives context information pertaining to the MN. In general, both authentication and RSVP context needs to be transferred to the new AP. RSVP context contains information about the traffic characteristics and QoS requirements of all the active sessions of the MN. Since the new AP might be running out of resources, an admission control algorithm decides which sessions can be maintained. The results of the admission control are transmitted to the old AP through the *MOVE-Accept* message and to the MN through the *ACCEPTED-Request* message. If the results of the admission control are acceptable to the MN, it responds back to the old AP with a positive *ACCEPTED-Response* message, and then switches to the new AP waiting for the handover procedure to finish. Otherwise, the answer is negative and the MN should try to handover to another AP, provided there is one available. In case of a positive answer, the old AP issues a positive *MN-Response* message to the new AP, in order to switch the data path (through a *Layer-2 Update Frame*) and start the RSVP signaling with the CNs of the accepted sessions.

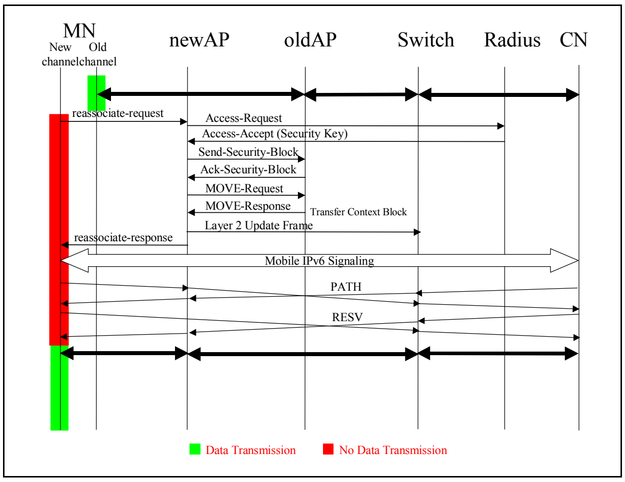


Figure 2. IAPP and RSVP standard message exchange

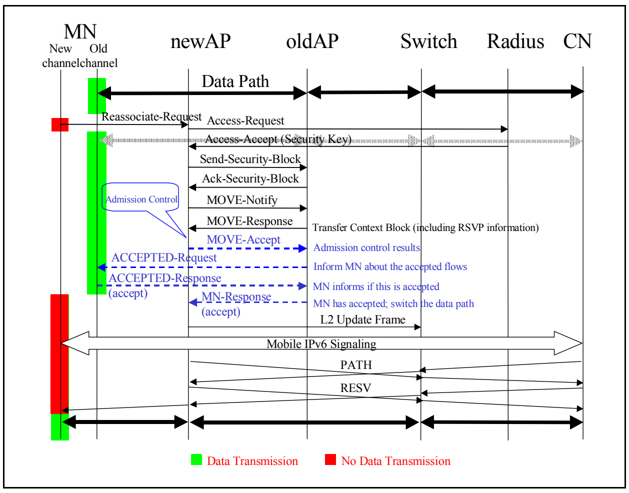


Figure 3. The proposed scheme

For an outgoing session, the MN can start transmitting data as soon as it receives the RSVP RESV message from the CN, while for an incoming session, the MN can simply wait to receive data packets. In this way, the MN does not have to cease transmission until the IAPP signaling is over, but it is allowed to use the old AP during this time. Additionally, the new AP acts as a proxy of the MN for the required RSVP signaling, reducing the path re-establishment time.

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).

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].

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.

V. Simulation Model and Numerical Results

To obtain numerical results and quantify the improvement attained with the use of the proposed scheme, a simulation model was developed focusing on modeling the message exchange between the involved nodes during handover. The simulation model was implemented with the OPNET tool [6], which offers appropriate mechanisms for the development of a platform for the functional and performance simulation of network architectures. The aim was to compare the proposed scheme (referred to as the IAPP+ scheme) with the conventional path re-establishment procedure during handover (referred to as the NO IAPP scheme), as well as a proposal made in [4] that uses IAPP to transmit RSVP information without changing the standard message exchange (referred to as the IAPP scheme). Comparison was made in terms of path re-establishment delays, under different traffic conditions in the radio interface. In order to focus on the interactions of the involved entities, a modeling approach according to [7] was followed to represent both the entities and the underlying transport network infrastructure (in the radio interface as well as within the distribution system).

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+……-+-+
|      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

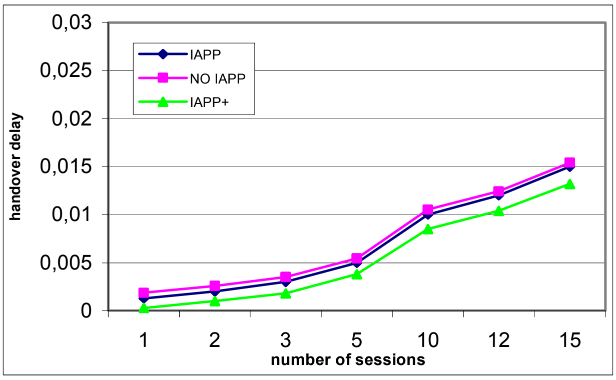
The simulation model included:

- the *"observed"* Mobile Node (MN), that represents the origination of signaling for outgoing RSVP sessions,
- the Corresponding Node (CN), that connects to the distribution system and represents the origination of signaling for incoming RSVP sessions,
- two Access Points (APs), between which consecutive handovers of the MN were performed, and
- a variable number of *"background"* MNs in the cell of each AP, generating the background (or interfering) traffic on the radio interface.

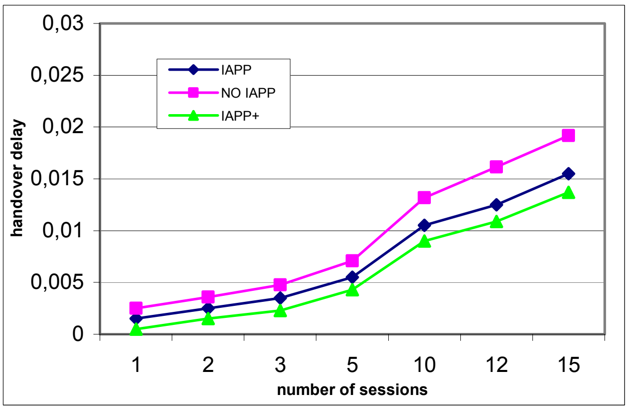
The AP and MNs in each cell were operating based on IEEE 802.11b in Distributed Coordination Function mode, with a bit rate of 11Mbps, while the two APs were connected through a fixed link of 100Mbps. Depending on the scheme under consideration (IAPP+, IAPP or NO IAPP), the execution of the corresponding message exchange was modeled separately. Three different levels of mean background traffic were considered in every cell, corresponding to 10%, 50%, and 80% of the maximum WLAN loading. For each level of background traffic load, several simulation runs were performed for different numbers of active sessions in the observed MN. In every run, the sessions were equally divided between incoming and outgoing, while a large number of handovers were executed in order to obtain accurate mean values.

The mean total path re-establishment delay for different numbers of sessions at the observed MN is illustrated in Figures 6 and 7, for incoming and outgoing sessions respectively. As can be observed, the improvement attained with IAPP and IAPP+ scheme is greater for incoming sessions, since both PATH and RESV messages are avoided over the radio interface. On the contrary, only the PATH message is avoided for outgoing sessions. In all cases, the delay improvement of the IAPP and IAPP+ scheme increases with the number of active sessions at the MN, as more messages are not transmitted on the radio interface. With the improvement added in the IAPP+ scheme, the data blocking time due to handover is reduced, leading to lower handover delay. As expected, the improvement from the use of the IAPP+ scheme is relatively the same, independently of the traffic load and the number of active sessions at the observed MN. This is because, as shown in Figures 2 and 3, the part of blocking time that is saved (IAPP signaling transmission at the fixed network), is not effected significantly by the traffic load.

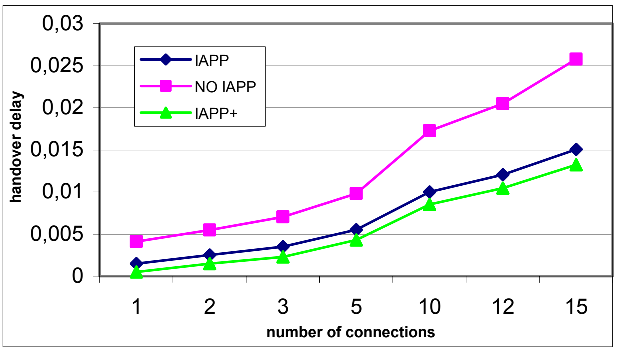
The amount of signaling overhead on the radio interface that is saved with the use of both IAPP and IAPP+ schemes, can be calculated as follows. As already mentioned, for every outgoing session only the PATH message is avoided, while for every incoming session, both the PATH and RESV messages can be avoided in the radio interface. Although the lengths of PATH and RESV messages are variable, there are a number of mandatory objects in every message. According to the length of the mandatory fields described in [3], it can be shown that the proposed scheme saves at least 124 bytes for every PATH message and at least 120 bytes for every RESV message that is not transmitted on the radio interface. Accordingly, the proposed scheme saves at least 244 bytes of signaling overhead on the radio interface for every incoming session and at least 120 bytes for every outgoing session. In Table 1, indicative gain of signaling overhead in the radio interface for different number of incoming and outgoing sessions is given.



(a) Traffic load equal to 10%

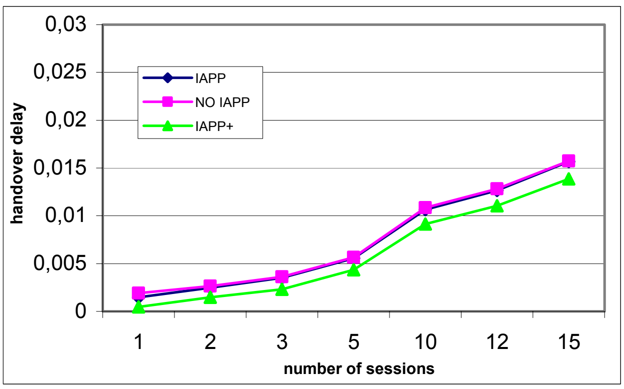


(b) Traffic load equal to 50%

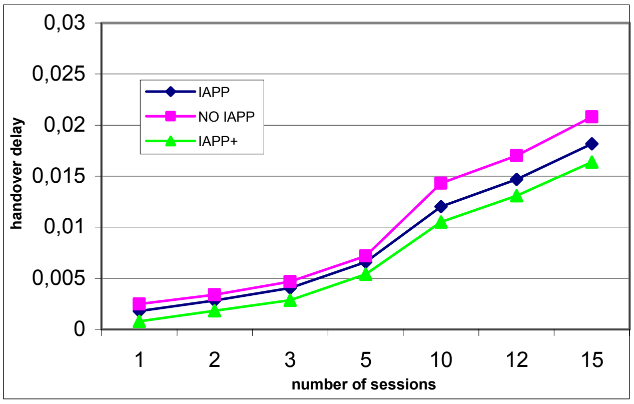


(c) Traffic load equal to 80%

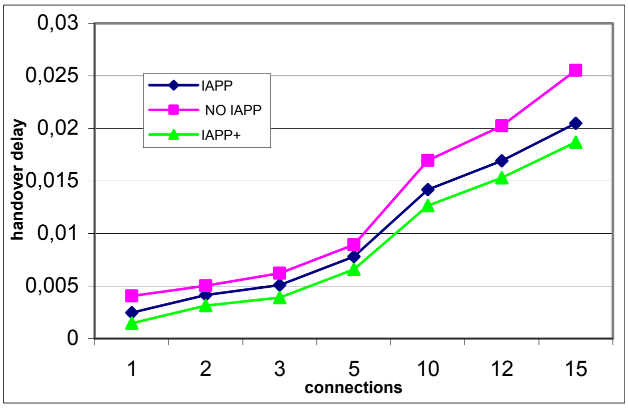
Figure 6. Path re-establishment delay for incoming sessions



(a) Traffic load equal to 10%



(b) Traffic load equal to 50%



(c) Traffic load equal to 80%

Figure 7. Path re-establishment delay for outgoing sessions

VI. Conclusions

In this paper, we studied a novel scheme that exploits IAPP in order to expedite RSVP path re-establishment in wireless LANs. In this context, we discussed the RSVP context that needs to be transferred across two APs with appropriate IAPP Information Elements, and we demonstrated how this context enables the new AP to initiate the required RSVP signaling on behalf of the MN. In addition, it was justified with simulation results that the proposed scheme can reduce both handover latency and signaling overhead on the wireless medium, especially in high traffic conditions. Future plans include the introduction of an 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 AP is insufficient to support the full set of active MN sessions. The decision should be based on factors such as session priority, traffic and QoS requirements, bandwidth utilization, etc.

#incoming RSVP sessions	signaling overhead gain (bytes)	#outgoing RSVP sessions	signaling overhead gain (bytes)
1	244	1	124
2	488	2	248
3	732	3	372
4	976	4	496
5	1220	5	620
6	1464	6	744
7	1708	7	868
8	1952	8	992
9	2196	9	1116
10	2440	10	1240

Table 1. Signaling overhead gain with the use of the proposed scheme

Acknowledgement

Part of this work was performed in the context of the project entitled "Always Best Connected Provision in Heterogeneous Mobile Networks" funded by the Greek Ministy of Education under the framework "Pythagoras".

References

[1] 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", January 2003.

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

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

[4] A. Salkintzis and N. Passas, "A New Approach for Fast Handovers in Mobile Multimedia Networks", Proc. IEEE Vehicular Technology Conference (VTC) Spring 2004, Milano, Italy, May 2004.

[5] C. Rigney et al., "Remote Authentication Dial In User Service (RADIUS)," RFC 2865, June 2000.

[6] OPNET Modeller Version 9.0, OPNET Web Site: http://www.opnet.com.

[7] G. Fleming, A. El-Hoiydi, J. DeVriendt, G. Nikolaidis, F. Piolini, and M. Maraki: "A flexible Architecture for UMTS", IEEE Personal Communications Magazine, April 1998.