Performance Improvement of Media Point Network using the Inter Access Point Protocol according to IEEE 802.11f

Ian Herwono[1], Joachim Sachs[2], Ralf Keller[2]
[1]Communication Networks, RWTH Aachen University, Aachen, Germany
[2]Ericsson GmbH, Eurolab R&D, Herzogenrath, Germany
e-mail: Ian.Herwono@comnets.rwth-aachen.de, {Joachim.Sachs | Ralf.Keller}@ericsson.com

Abstract – **This paper demonstrates how the Inter Access Point Protocol (IAPP) can be used to improve the performance in a Media Point systems. The Media Point system [1-6] provides high-volume personalized data services within WLAN hotspots with discontiguous coverage areas. Based on our experimental performance evaluation [4-6] we present three mechanism to improve performance. First, IAPP allows to reduce the required signalling by means of an extended EAP-TLS authentication procedure. Second, IAPP can be used to trigger an abbreviated DHCP procedure. Third, we present a pre-caching mechanism for the hierarchically structured media point network. In the latter two mechanisms the role of IAPP is to provide the terminal MAC address to other Media Point control nodes.**

1. Introduction

The concept of Media Point on the provisioning of personalized high bit-rate multimedia data to users within a WLAN environment was introduced in [1-4]. The selected mechanisms and protocols have been implemented in a demonstrator system and an experimental performance evaluation has been carried out [4-6]. As depicted in Fig. 1, in the Media Point architecture the WLAN Access Points, i.e., the Media Points (MP), are controlled by a number of Media Point Controllers (MPCs), that in turn are controlled by a central Media Point Service Control (MPSC). The IETF Session Initiation Protocol (SIP) is used to control the service provisioning and to deal with the mobility management. The current user's presence status is monitored by the SIP Presence Server (PS), which is co-located with the MPSC.

One main requirement of the Media Point service concept is the need for a fast and reliable setup of the data communication session when a user terminal enters a hotspot area (of an MP). If the user is moving and leaving the hotspot, the Media Point core network should ensure that the (interrupted) session can be resumed at another MP "smoothly" and without high delays. As pointed out in [4-6] many factors influence the duration of session setup and resume procedure, such as the station association with the MP, the chosen method and parameters of the DHCP (Dynamic Host Configuration Protocol) procedure, or the amount of data to be cached in the particular service node. One approach is to allow an exchange of information, which is specific to the user's communication session, i.e., context transfer, between the new and the old access node.

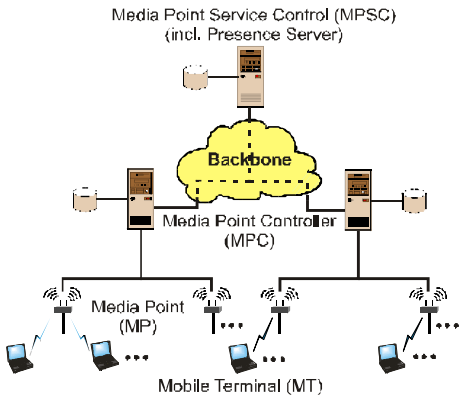

Fig. 1. Media Point network architecture

In this paper we investigate such context transfer approach within the WLAN environment by analyzing the Inter Access Point Protocol (IAPP) which has been specified by the IEEE 802.11f working group. Our main goal is to determine to which extent IAPP can improve the Media Point system performance in terms of reduced session setup and resume times. We provide a summary of the features and functionalities of IAPP on achieving the interoperability between multi-vendor access points and supporting re-authentication of roaming stations according to the IEEE 802.1x standard. We present and discuss our proposals on making use of standard IAPP mechanisms in the Media Point network environment for the performance improvement afterwards.

2. The Inter Access Point Protocol (IAPP) of IEEE 802.11f

2.1. Protocol Overview

The Inter Access Point Protocol (IAPP) [7] aims to achieve multi-vendor access point interoperability within a Distribution System (DS). In 802.11 terminology, a DS is a system used to interconnect a set of Basic Service Sets (BSSs) and integrated Local Area Networks (LANs) to create an Extended Service Set (ESS). An Access Point (AP) is a station (STA) that provides other stations access to the DS (by providing DS services). A BSS is a set of stations (STAs) controlled by an AP (within an infrastructure-based WLAN), while an ESS is a set of one or more interconnected BSSs and integrated LANs, that appears as a single BSS to the Logical Link Control (LLC) layer at any station associated with one of those BSSs [8].

While the MAC (Medium Access Control) and PHY (Physical) layers of a WLAN system are specified in IEEE 802.11 standard, the implementation of the concepts of APs and DSs is not standardized. Physical

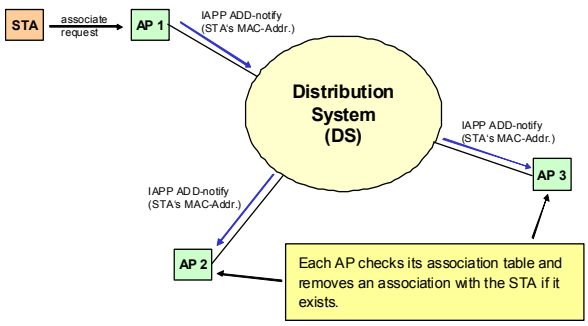

Fig. 2. Enforcing single station association with IAPP ADD-notify packet

AP devices of different vendors are thus unlikely to interoperate across a DS. IAPP deals primarily with this interoperability issue. IAPP is a communication protocol, used by the AP Management Entity (APME) to communicate with other APs, when various local events, e.g., station association, occur in the AP.

IAPP allows a secure exchange of station context information between APs and thus sharing of authentication data. While roaming, i.e., moving between APs, the mobile station might thus not need to re-authenticate at the backend authentication server, e.g., a RADIUS server, anymore. This will reduce the load on the server and speed up the roaming/handover procedure while enabling seamless connectivity at the same time.

However the most complete services of IAPP can only be provided to the APs if a station makes use of the *Reassociation Request* frame when roaming from one AP to another. When the *Association Request* is used instead, it is not possible for IAPP to notify the AP, with which the station was last associated, of the new association (at the new AP). This disables the possibility to transfer the station context information from the old to the new AP and will result in a (time consuming) re-authentication of the station. The Association Request only allows IAPP to enforce single association of a station within the subnet domain at any given time.

2.2. IAPP Operation Triggered by Station Association

When a station associates with an AP using Association Request frame, the corresponding AP's IAPP entity will generate a *Layer 2 Update frame* and an *IAPP ADD-notify* packet. The Layer 2 Update frame is sent to the DS to cause the forwarding tables in any layer 2 devices that receive the frame to be updated so that all future traffic received by those bridges/switches is forwarded to the port on which the frame was received. The IAPP ADD-notify packet is used to notify all APs in the local broadcast domain of the DS of the (new) association between the AP and station. The IAPP entity sends the packet to the subnet limited broadcast address using UDP/IP. In particular, the IAPP ADD-notify packet carries the MAC address and a sequence number from the associating mobile station. The sequence number should indicate the recentness of the association request.

After successfully sending Layer 2 Update frame and IAPP ADD-notify packet, the IAPP entity notifies the APME (AP Management Entity) to provide DS services (of the AP) to the station. Note that the IAPP entity does not expect any response from other APs in the DS that have received the broadcast IAPP ADD-notify packet.

When an IAPP ADD-notify packet is received by an AP from the DS, its IAPP entity notifies the overlying APME about an association relationship between a mobile station and another AP in the DS. In case that the station is still associated with the AP, its APME should disassociate this station. This way a single association of a mobile station in the DS can be achieved. The included sequence number ensures that only the newest association request from the station will be considered. Fig. 2 depicts the scenario in which one mobile station (STA) associates with an AP (AP1) which is interconnected through a DS with two another APs.

2.3. IAPP Operation Triggered by Station Reassociation

When a station reassociates with the AP using a Reassociation Request frame the corresponding IAPP entity will cause a Layer 2 Update frame to be sent to the DS which will update forwarding tables in any layer 2 devices, too. A reassociation request is sent when the station wants to indicate with which AP it was associated previously. Hence, together with the station's MAC address and a sequence number, the MAC address of the old AP, that is obtained from the *Current AP Address* field of the Reassociation Request frame, is provided to the new AP.

In summary, upon receipt of the Reassociation Request frame the IAPP entity (of the new AP) should take the following actions:

1. Determination of the DSM (DS Medium) layer 3 address (i.e., IP address) associated with the BSSID of the old AP presented in the Reassociation Request frame
2. Determination and retrieval of security parameters needed to establish secure channel between the APs
3. Sending a Layer 2 Update frame to the DS to update the forwarding tables in any receiving bridges/switches
4. Sending an IAPP MOVE-notify packet via TCP/IP to the old AP to request context information of the station that has just associated with the (new) AP; the packet is addressed using the IP address of the old AP

In order to determine the old AP's IP address and the security parameters, the use of RADIUS (Remote Authentication Dial In User Service) protocol [9] is recommended. The message exchange with the RADIUS server (also connected to the DS) must take place first before the IAPP MOVE-notify packet can be transferred via TCP/IP. It is also to obtain the information from a trusted party, i.e., the RADIUS server, whether the old AP, with which the station was associated, is a valid member of the ESS of the new AP

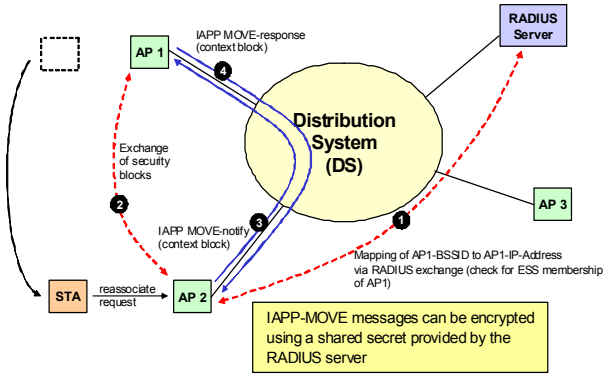

Fig. 3. Context transfer from an old AP (AP 1) to new AP (AP2) due to station reassociation

(new BSSID); hence, whether the communication (i.e., context transfer) between both APs is allowed and can take place securely. The new AP sends an Access-Request packet containing the old AP's BSSID, to the RADIUS server. In case of successful verification of the ESS membership the RADIUS server responds with an Access-Accept packet, which includes the old AP's IP address. A secure channel between the APs can optionally be established for the subsequent context transfer.

After the secure channel is established or upon receipt of the Access-Accept packet the IAPP entity (of the new AP) sends the IAPP MOVE-notify packet to the old AP (using its IP address) via TCP/IP. The packet carries the MAC address and sequence number of the reassociating station. The old AP should forward any relevant context information of the reassociating station to the new AP within the *IAPP MOVE-response* packet using TCP/IP. This IAPP packet differs from the IAPP MOVE-notify packet only in the status field whose value is either "0" (successful) or "1" (stale move). Stale move status means that the old AP has a current association with the specified station with a more recent sequence number than the one indicated by the IAPP MOVE-notify packet. When the new AP receives the IAPP MOVE-response packet with a successful status it should cause the DS services to be provided to the reassociating station. Otherwise the new AP should disassociate the station. This might happen, for example, when the station has successfully reassociated with the "old AP" again before the "old AP" receives the IAPP MOVE-notify packet from the "new AP". Fig. 3 depicts the scenario in which the mobile station (STA) reassociates with AP2 after it was associated with AP1 previously.

2.4. EAP-TLS Authentication with IAPP Support

EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) provides a mechanism for certificate based mutual authentication, together with the establishment of a session key at the station and the RADIUS server according to the IEEE 802.1x standard [10]. The session key is used by the AP to securely distribute the WEP (Wired Equivalent Privacy) encryption keys to the stations associated with the AP. As the station (or its user) and the RADIUS server are identified by their public-key certificates, a certificate distribution and management system, i.e., PKI (Public Key Infrastructure), is required. The EAP-TLS protocol assumes that the certificates have been obtained from trusted third parties and already stored by their owners.

In case of roaming stations it is obvious that a re-authentication at the new AP requires much authentication data to be exchanged between the station and the RADIUS server (relayed by the AP). This could delay the roaming/handover procedure and result in interruption of ongoing data communication sessions. IAPP deals with this issue by using its context transfer

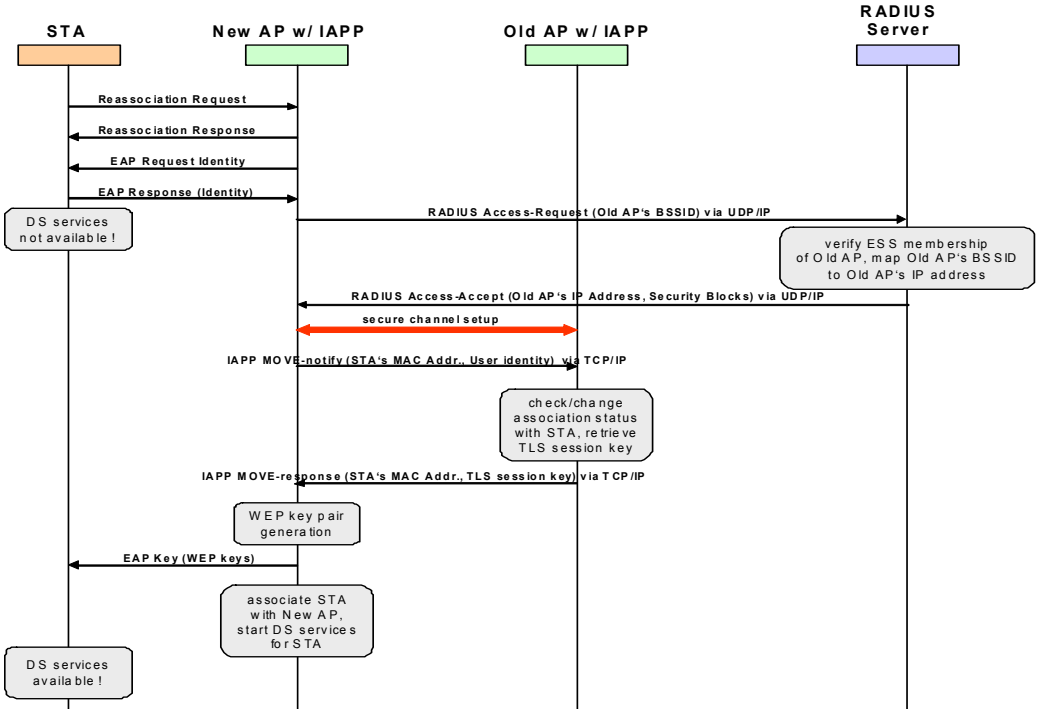

Fig. 4. EAP-TLS re-authentication with IAPP support during station reassociation

capability to exchange the authentication data between the APs.

The goal of IAPP is to minimize the communication traffic between the roaming station, the AP and the Authentication Server (RADIUS server) while keeping the established security association between the parties intact. Provided that the mobile station (STA) sends a Reassociation Request frame when roaming to the new AP, the new AP sends an *EAP Request Identity* frame to STA, as shown in Fig. 4.

STA responds with its identity (machine- or username) in an *EAP Response* frame. After verifying the ESS membership of the old AP, determining its IP address and establishing a secure channel with the old AP, the new AP includes the EAP user identity in the IAPP MOVE-notify packet. When the old AP receives the IAPP MOVE-notify packet, it extracts the EAP user identity and determines the corresponding TLS session key that was generated during the previous authentication of STA with the RADIUS server and sent to the old AP. The old AP sends the TLS session key within the IAPP MOVE-response packet to the new AP over the secure channel. The new AP may then generate a new WEP key pair for STA, if necessary. The (new) WEP keys will then be encrypted using the TLS session key and sent to STA. STA can decrypt the message and extract the WEP keys as it owns the TLS session key, that was generated during its last EAP-TLS authentication with the RADIUS server via one of the previous APs. From this point in time STA can access the network via the new AP and perform link-layer data encryption with the new AP securely using new WEP encryption keys.

In contrast to standard EAP-TLS authentication, as much less data must now be exchanged between STA and the (new) AP, e.g., no client certificate should be transferred, and no STA authentication with the RADIUS server must be performed at all. The roaming/handover procedure can be accelerated. However, it has to be mentioned, that the IAPP procedure to support EAP-TLS authentication described above is not standardized yet. It should be seen as a proposal to avoid EAP-TLS re-authentication if IAPP should be used during station roaming/reassociation. The security aspects of such security context transfer procedure should be deeper investigated and analyzed in order to determine which context information is mandatory to be exchanged, which security measures should be taken and which security level can be offered.

3. IAPP in the Media Point Network

In this section we discuss the use of standard IAPP mechanisms to support the multi access point management within a WLAN based Media Point network with regard to the following issues:

- How can IAPP be integrated into a Media Point system for multi access point management ?
- To which extent can IAPP improve the system performance regarding the session setup or resume time ?
- How much effort is required to achieve the system improvement when using IAPP ?

The implementation of a Media Point system demonstrator described in [4-6] is used as a reference for our further consideration in conjunction with the IAPP. The demonstrator setup is shown in Fig. 5. As pointed out in [4-6] two factors significantly influence the delays in the session setup and resume times are:

1. The implemented DHCP (Dynamic Host Configuration Protocol) mechanism for assigning an IP address to stations needs up to one second to complete while at the same time producing inordinate load on the station and the DHCP server (i.e., MPC) due to very short address refresh interval (i.e., client daemon mode).
2. Due to data caching in the serving MPC, the data transfer to the station will be delayed to a certain degree depending on how much personalized multimedia data to cache.

Furthermore the time needed by the station to associate with an AP has been measured to be on average 1.6 seconds, which actually takes more than the half of the total session setup time (without data caching). As IAPP operates first after a successful association, no improvement regarding association time can be achieved.

3.1. Station Association in the Media Point Network

As during a station association with an AP no information about the old AP (if any) is provided to the new AP, no context transfer between the APs can be executed by means of IAPP. The aim in this scenario is to determine whether IAPP operations can somehow support the Media Point system to minimize the occurring delays.

3.1.1. Reduction of DHCP procedure time

After a station has successfully associated with an AP, the station must be assigned an IP address via DHCP. A DHCP procedure is started with a *Discover* message broadcast by the client (station) to contact a DHCP server, which in turn can offer an IP address. In the Media Point environment the DHCP server is installed in each MPC. In the demonstrator the station must send the Discover message periodically as long as no answer from a DHCP server is received. Since the point in time, at which a successful station association is completed, might be within the interval time between two Discover messages, a delay occurs until the DHCP

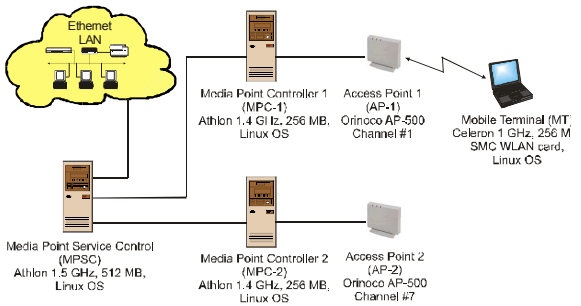

Fig. 5. Setup of the Media Point demonstrator

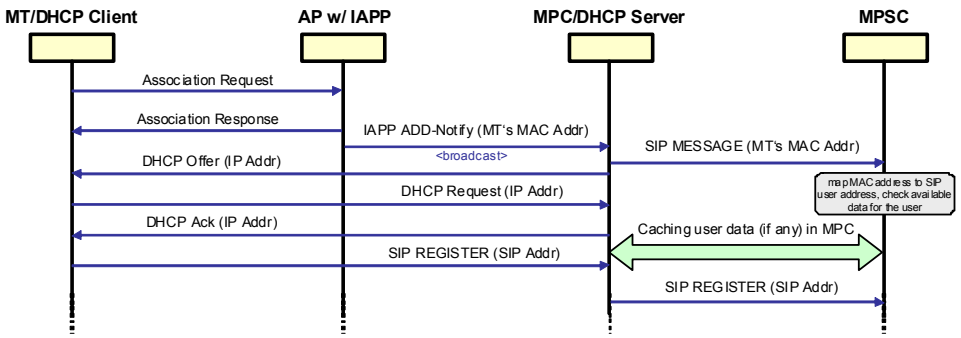

Fig. 6. IAPP support for triggering DHCP procedure and data caching in MPC within a Media Point network during station association

procedure can be started. The minimum DHCP Discover interval time (i.e., one second) is thus set in the demonstrator which results in an average delay (i.e., idle time) of 0.5 second. The drawback of this approach is that the station will waste its resources to broadcast unneeded Discover messages in case that the station is not associated with an AP at all. When the DHCP procedure should be triggered by a successful association, we observed a delay of up to four seconds in case that no modification of the used DHCP client software is made.

Our proposal is to release the station from trying to discover a DHCP server at any given time; the DHCP procedure will instead be started by the DHCP server itself. Hence the procedure is started with a DHCP Offer message containing an offered IP address. This non-standard procedure requires modification of the DHCP server software.

In order to allow sending the Offer message to the station that has successfully associated with the AP (which is connected with the MPC acting as a DHCP server), the station's MAC address is needed. This MAC address is included in the broadcast IAPP ADD-notify packet and should be extracted by the receiving MPC, as depicted in Fig. 6. The DHCP server uses the station's MAC address as the destination address of its Offer message. In turn the DHCP client software (at the station) must also be modified to be ready to receive and process an Offer message without having to send a Discover message first. Upon receipt of the Offer message the station can then perform the standard DHCP procedure by responding with a *Request* message indicating that it agrees to use the offered IP address. By using this approach we expect a reduction of DHCP procedure time of up to 0.5 second and a significant decrease of the client system load.

3.1.2. Reduction of MPC data caching time

Upon completion of the DHCP procedure the station sends a *SIP REGISTER* message to the MPC (functioning as a SIP Proxy Server) to announce the presence of a particular SIP user. The MPC relays this REGISTER message to the MPSC which then checks whether there is any personalized data available for the user. If yes, the serving MPC caches then the data before transferring it to the station. Depending on the amount of data (and the current transmission characteristics between MPC and MPSC) this caching process may take several seconds to complete [4-6].

To minimize the waiting time, appropriate pre-caching mechanisms and strategies have to be applied. With support of IAPP the caching process might already be started before the station sends a REGISTER message. After receiving the IAPP ADD-notify packet, the MPC has the knowledge of the station's MAC address but not the particular user's SIP address. To start the caching procedure, a mapping of the station's MAC address to the corresponding SIP user address has to be done first. We assume that the MPC will not be able to do this mapping by itself and thus needs to contact a central entity like an MPSC. Indeed there are several ways to realize this mapping. One approach is to send the MPSC a *SIP MESSAGE* indicating the need for MAC/SIP address mapping, as shown in Fig. 6. Another approach is to use a RADIUS server to do the mapping, which might cause additional delay.

When the MPSC approach is used, the MPSC must maintain a database, which maps a MAC address to the corresponding SIP user address or a group of them. This is due to the fact that several users might use the same station with a unique MAC address. When the SIP user address has been identified the MPSC can check whether or not there is any personalized data available for the user and initiate the caching procedure with the MPC accordingly. After the station is assigned an IP address, it sends the REGISTER message to the MPC and must wait for a shorter time until it can download the user data from the MPC via the AP. Note that this approach can reduce the download waiting time significantly only if unambiguous mapping of the MAC/SIP address can be ensured. In case that an extended authentication like the EAP-TLS described in Section 2.4 can be employed, the SIP user address might be included in the user's public-key certificate to be exchanged with the RADIUS server (i.e., MPSC). An unambiguous mapping of MAC/SIP address can thus be achieved and the MPC caching procedure can be started by the MPSC as soon as possible.

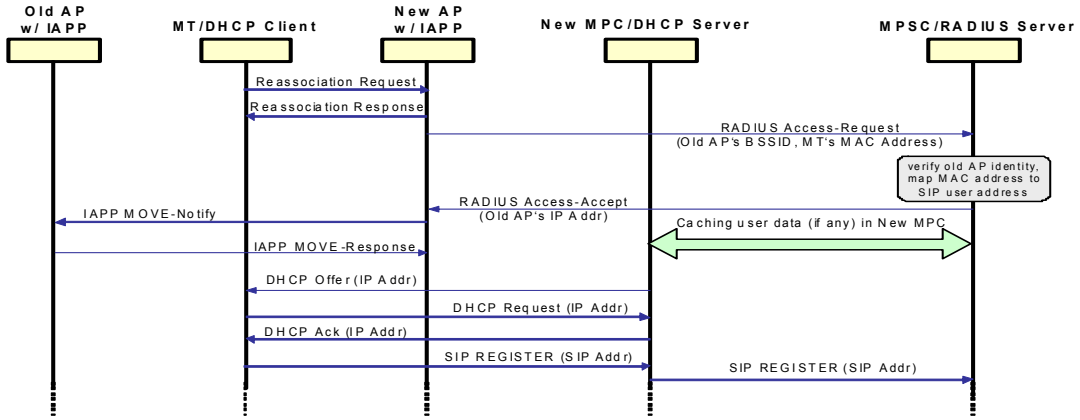

Fig. 7. IAPP support for triggering DHCP procedure and data caching in MPC within a Media Point network during station reassociation

3.2. Station Reassociation in the Media Point Network

When a station reassociates with a new AP, the new AP receives information about the (old) AP with which the station was last associated and can therefore execute a context transfer. After verifying the ESS membership and determining the IP address of the old AP, the new AP sends the old AP an IAPP MOVE-notify packet containing among others the station's MAC address. Since it is not a broadcast packet and it cannot be received by the MPC/DHCP server, which wants to extract and use the station's MAC address for triggering the DHCP procedure.

The point is that in our current Media Point system implementation all possible context information like the SIP user address or the current level of downloaded data is stored in MPC and context transfer should therefore be performed between the MPCs or between MPC and MPSC. Such context transfer is useful when the station moves to a new AP which is controlled by another MPC (i.e., inter MPC handover). As standard IAPP operations only support context transfer between the APs, the context information must also be stored in each AP. To make use of the context transfer capability of IAPP, additional non-standard Media Point specific entity should be integrated in the AP architecture. This entity stores some context information like the SIP user address (in conjunction with the MAC address of the used station) and has an interface to the IAPP entity to allow it use the IAPP services to exchange the Media Point specific context information with other APs. This AP's Media Point entity should also be able to communicate with an MPC using an appropriate data exchange protocol. Obviously the drawback of this approach is that high effort to implement such Media Point entity in each AP is needed and the interworking between APs of different vendors cannot be guaranteed as long as it is not standardized.

The only possibility to avoid the necessity of an additional protocol entity within the AP is to include more information or attributes in the RADIUS Access-Request message, which is sent by the new AP to verify the identity of the old AP during station reassociation. In the IAPP standard document this RADIUS message includes the name of the user to be authenticated or checked, which is the BSSID of the old AP. Other identity information relates to the identity of the new AP, such as the new AP's IP address or the new AP's MAC address (included as the attribute *Called-Station-Id*). However, RADIUS defines an optional attribute named *Calling-Station-Id* which refers to the phone number that the call came from [9]. This attribute is not used by IAPP for its RADIUS Access-Request message. In the Media Point system we propose to include the MAC address of the station as the Calling-Station-Id attribute in the Access-Request message, in order to provide the RADIUS server the information about the station's identity (Fig. 7).

Upon receipt of the Access-Request message the RADIUS server (i.e., MPSC) proceeds with the standard verification procedure for the particular old AP and additionally consults its database to map the station's MAC address to the corresponding SIP user address. Since the database is updated regularly based on previous communications with the controlled MPCs and the MPSC, the MPSC can determine with which MPC the station was last connected (according to the IP address of the old AP connected to the MPC). An unambiguous mapping of station's MAC address to the particular SIP user can thus be made. By knowing the IP address of the new AP the RADIUS server can determine the new serving MPC as well. If any personalized data for the SIP user is available at MPSC, the caching procedure with the new MPC can be started immediately. This may also trigger the new MPC to initiate a DHCP procedure with the reassociating station by sending it an Offer message. The station's MAC address can be included within a separate SIP message (using MESSAGE method) or within the *SIP INVITE* message sent by the MPSC to start the caching procedure. However, it could be possible that the station must wait until it is allowed to use the DS services before the station can reply the MPC with a DHCP Request message. The DS services are started by the new AP after the standard IAPP reassociation procedure is completed (exchange of IAPP MOVE-notify/response packets with the old AP). We currently see no requirement for the IAPP to carry any Media Point specific context information from the old to the

new AP. This IAPP context transfer feature will be used especially when extended authentication method like EAP-TLS is employed for AP access control.

4. Conclusions

In this paper we have analyzed the capability of the Inter Access Point Protocol (IAPP) – specified by the IEEE 802.11f working group – to reduce the session setup and resume times in a WLAN based Media Point network. IAPP provides mechanisms to support the interoperability and context transfer between Access Points (APs) of different vendors, which is required when stations are moving and roaming between different APs. IAPP operations that are triggered by a station association, can force a single association of particular station within the WLAN subnet.

Within a Media Point system the Media Point network is managed in an hierarchical structure of Media Point Controllers (incl. DHCP functionality) and Media Point Service Controller (incl. SIP Presence Server, RADIUS server). As a consequence most Media Point related context is not located in the AP but rather in MPC and MPSC, yielding only limited gain to IAPP based context transfer between APs. One procedure where IAPP could provide benefit is a new extended authentication scheme for EAP-TLS to reduce roaming or handover time. For context transfer between e.g. MPCs IAPP is not suitable and other protocols such as IETF Context Transfer Protocol (CTP) [11] should be preferred.

In previous work [4-6] it has been demonstrated that the performance of the Media Point system is mainly limited by two procedures, the IP address assignment of DHCP and data caching in MPC. In this paper we have proposed a solution how IAPP can be used to improve these two procedures.

The DHCP procedure can be improved if it is not initiated from the mobile station but instead by the DHCP server when the mobile station associates with an AP. For these changes it is however required, that the mobile station MAC address gets known in the DHCP Server (located in MPC). In order to improve the data caching procedure user data is already forwarded to the new serving MPC during the connection procedures of the mobile station. For that it is required that the MPSC maintains an unambiguous mapping of the user SIP URL and its MAC address. In addition it is required that the mobile station MAC address is provided to the MPSC, as well as the IP address of the new serving MPC. The latter can be derived from the IP address of the new AP. In this paper we have demonstrated two procedures of how IAPP can be used to trigger these procedures and transport the required information. The first procedure describes the normal case that the mobile station associates at a new AP. The second procedure further assumes that the AP reassociation procedure of 802.11f in combination with extended EAP-TLS authentication is used.

While we have not implemented the new mechanisms in our prototype, we argue that the following gain can be achieved compared to the results obtained in previous work [4-6]. The gain of extended EAP-TLS reduces the amount of signalling required to set up a new connection. The gain of the pre-caching mechanism depends largely on the characteristics of the data session. In the best case it will reduce the session resume time by the time required to transmit all user data from MPSC to MPC. For the DHCP procedure, the new mechanism will allow to save approx. 0.5 s and at the same time largely reduce the DHCP load of broadcasted DCHP Discover/Offer messages.

ACKNOWLEDGMENT

The work presented in this paper has been partly supported by the German Federal Ministry of Education and Research in the project "IPonAir" (01BU163).

REFERENCES

[1] B. Walke, J. Habetha, I. Herwono, R. Pabst, D.C. Schultz, *"The Wireless Media System: A Mobile Broadband System with Invisible Infrastructure and Low Radio Exposure of Humans"*, In Proceedings of the ANWIRE 1st International Workshop on "WIRELESS, MOBILE & ALWAYS BEST CONNECTED", University of Strathclyde, Glasgow, April 2003.

[2] B. Walke, I. Herwono, R. Pabst, *"Service Architecture for Infrastructure based Multi-hop Networks based on SIP"*, In Proceedings of ICCT 2003 International Conference on Communication Technology, April 2003.

[3] G. Plitsis, R. Keller, J. Sachs, *"Realization of a Push Service for Media Points based on SIP"*, In Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks, Stockholm, Sweden, September 2002.

[4] I. Herwono, J. Sachs, R. Keller, "*Provisioning and Performance of Mobility-Aware Personalized Push Services in Wireless Broadband Hotspots*", to appear in Computer Networks Journal, 2005.

[5] I. Herwono, J. Sachs, R. Keller, *"A Prototype for the Provision of Mobility-Aware Personalized Services in Wireless Broadband Hotspots"*, In Proc. Fifth European Wireless Conference (EW 2004), Barcelona, Spain, February 24-27, 2004.

[6] I. Herwono, S. Goebbels, J. Sachs, R. Keller, *"Evaluation of Mobility-Aware Personalized Services in Wireless Broad-band Hotspots"*, In Proc. Communication Networks and Distributed Systems Modelling and Simulation Conference, San Diego, California, USA, January 18-21, 2004.

[7] IEEE Standards 802.11f/D5, *"Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11 Operation"*, January 2003.

[8] IEEE Standards 802.11, *"Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications"*, 1999.

[9] C. Rigney, A. Rubens, W. Simpson, S. Willens, *"Remote Authentication Dial In User Service (RADIUS)"*, RFC 2865, June 2000.

[10] ORiNOCO Technical Bulletin 048/B, *"Principles of 802.1x Security"*, April 2002.

[11] J. Loughney et al., *"Context Transfer Protocol"*, Internet Draft, Seamoby WG, Internet Engineering Task Force, August 2004.