Wireless Netw (2007) 13:497–510
DOI 10.1007/s11276-006-9202-6

Improvements on "IP – IAPP": A fast IP handoff protocol for IEEE 802.11 wireless and mobile clients

Ioanna Samprakou · Christos J. Bouras · Theodore Karoubalis

Published online: 15 June 2006

Abstract One of the most critical issues in introducing Wireless LAN (WLAN) real-time and delay sensitive applications, such as Voice over IP (VoIP), is guaranteeing IP service continuation during inter-subnet Basic Service Set (BSS) transitions. Even though WLANs offer very high channel bandwidth, they exhibit long network-layer handoff latency. This is a restraining factor for mobile clients using interactive multimedia applications such as VoIP or video streaming. In a previous work, we presented a novel fast and efficient IP mobility solution, called "IP-IAPP", which offers constant IP connectivity to the 802.11 mobile users and successfully preserves their ongoing sessions, even during subnet handoffs (fast recovery of active connections). It is an 802.11-dependent IP mobility solution, which accelerates the network reconfiguration phase after subnet handoffs and significantly reduces the IP handoff latency. It restores L3 connectivity almost simultaneously to the L2 connectivity after a subnet handoff, due to a zero-delay movement detection method. As a result, even the most demanding next generation WLAN applications such as Voice over WLAN (VoWLAN) suffer insignificant disruption. In this paper we present an improved version of the IP-IAPP mobility mechanism (new optimized protocol procedures). Certain extensions have also been incorporated to the initial proposal, for the provision of more advanced services: (a) secure inter-AP IP-IAPP communications, (b) zero patching on the clients s/w, and (c) support of clients which use a dynamic IP address. Performance measurements out of further and more complex testing verify that the proposed method outperforms other existing mobility solutions, and still introduces the lesser imperative amendments to the existing 802.11 wireless LAN framework.

Keywords 802.11 Wireless LANs · IAPP · IP mobility · Fast handoff · IP connectivity

1. Introduction

The IEEE 802.11 technology [7] is one of the most prevailing wireless communication options today. A critical and most discussed issue in the area of wireless communications is the handoff latency problem caused during roaming of the 802.11 wireless clients. The 802.11 clients need also be *mobile* as well as being wireless. Next generation applications running on wireless networks like VoIP, pose an emerging need to both provide users with the ability to remain IP connected and to quickly restore their ongoing sessions during any kind of movements (handoffs) inside WLANs. The network reconnection latency during intra-subnet handoff is solved by the existing IEEE 802.11f Inter-Access Point protocol (IAPP) [1]; however, no existing IEEE standard addresses the IP handoff issue. As a result, users suffer from great IP recovery periods during inter-subnet roaming (excessive latency

I. Samprakou
Department of Computer Engineering and Informatics,
University of Patras, Patras, Greece
e-mail: sampraku@ceid.upatras.gr
Atmel Hellas, MMC S.A., Athens, Greece
e-mail: isamprakou@athens.atmel.com

C. J. Bouras (✉)
Department of Computer Engineering and Informatics,
University of Patras, Patras, Greece
e-mail: bouras@ceid.upatras.gr
Research Academic Computer Technology Institute,
Patras, Greece
e-mail: bouras@cti.gr

T. Karoubalis
Atmel Hellas, MMC S.A., Athens, Greece
e-mail: tkaroubalis@athens.atmel.com

and jitter, degraded voice quality). There is an emerging need to optimize the time required to complete the inter-network BSS transitions of wireless clients. The key issues involved in a client's subnet movement include the roaming latency, the proper and fast adjustment of IP state information at the 802.11 Access Points (APs), the preservation of a client's ongoing sessions, and the ability to continue to be IP-connected regardless of its physical position.

In this paper we deal specifically with IP mobility of wireless clients in 802.11-based networks, in order to effectively support L3 handoffs which may occur in WLANs. We present an enhanced version of our previously proposed fast handoff method [8], named "IP-IAPP", which offers the 802.11 Mobile Nodes (MNs) unlimited mobility. The IP-IAPP protocol is built on top of the 802.11f IAPP and supports fast and reliable IP handover of wireless stations in WLAN environments. It aims to preserve the IP-flows of mobile nodes as they roam across different subnets. It extends WLAN roaming capabilities by offering uninterrupted service even to time critical applications. The basic feature of this approach is that it uses a modified 802.11f mechanism in the event of subnet handoffs. The 802.11f protocol is extended so that IAPP packets are also used to deliver information concerning the IP state (location) of the 802.11 MNs, and provide the involved APs with the means to deploy advanced routing setup regarding the L3-roaming enabled MNs. The distinction between a simple intra-network (L2) handoff and an inter-network (IP) handoff is executed at the APs, and if an IP handoff is identified, the IP-IAPP protocol procedures are immediately launched. Via the use of advanced IP-IP tunneling setup (IPv4 tunneling) established during network layer handoffs, the APs offer IP-connectivity to wireless clients always and everywhere. The APs which serve foreign MNs act as their Foreign Agent (FA); they handle all MNs' IP traffic for as long as they remain in the foreign network, while a dedicated AP inside the MN home network, the Home Agent (HA), serves as an anchor point for all MN traffic reaching the home network. What is achieved by this approach is the ability of 802.11 APs to offer *seamless* (total IP handover delay < 60 ms) and *smooth* L3 (IP) handoff support to the wireless and mobile 802.11 stations. Stations are able to roam freely to foreign networks (and connect to foreign APs), without observing any change in their IP connectivity status. As will be confirmed later by the test results, the proposed method quickly restores IP connectivity and successfully preserves the ongoing sessions, as the overall handover delay (L2 + L3) is insignificant, even for demanding and delay-sensitive applications.

The rest of the paper is organized as follows: In Section 2 we present some related work concerning network layer handoffs in wireless networks. Section 3 analytically presents the current version of the IP-IAPP fast IP handoff mechanism, along with an introduction of the new features incorporated to the standard IP-IAPP proposal for advanced services support. The performance results of the proposed IP mobility solution, based on real testing using IP-IAPP enabled 802.11 APs, follow on Section 4, while Section 5 concludes the paper.

2. Related work

Mobile IP (MIP) [2] is the widely used solution for the provision of host mobility, regardless of the underlying L2 technology. However, the significant MIP handoff delay (the movement detection process alone may range up to 3 seconds [17]) affects the service quality especially of multimedia applications, while it constitutes an inefficient solution for 802.11 systems. Several techniques have been proposed to optimize the MIP performance (long handover delays make MIP unable to preserve open IP sessions upon IP handovers) by either improving *MIP handoff latency*, or by optimizing *MIP routing*. There also exists a number of methods which try to support IP mobility in WLANs using a different approach than Mobile IP. Most of these mobility proposals (MIP optimization techniques, like Hierarchical MIP [6], and others) are L2 independent; this many times results in poor applicability of those approaches in 802.11 wireless frameworks, as will be argued later on this section.

In an effort to shorten the MIP movement detection phase, which is the decisive factor in the Mobile IP handoffs, [3] presents two Mobile IP *Advertisement-based* movement detection algorithms: (a) the *Eager Cell Switching (ECS)*, and (b) the *Lazy Cell Switching (LCS)*. The LCS method aims to avoid MIP handoff until they are absolutely necessary. The ECS algorithm tends to function in a way opposite to that of LCS. It assumes frequent location changes and therefore pursues immediate handoffs upon discovery of a mobility agent. The ECS based MIP handoffs complete faster than their LCS counterparts. Some interesting work on accelerating the MIP handoff delay is also presented in [15, 16], the *Hinted Cell Switching (HCS)* method. The HCS method is introduced as a new alternative to the Mobile IP *Advertisement-based* movement detection methods, which relies on *hints* generated during subnetwork layer handoffs for reacting faster to Mobile IP handoffs. In [14], an enhanced movement detection method for Mobile IP is introduced, called the Fast Hinted Cell Switching (FHCS). This method assumes that the link layer is capable of delivering information to Mobile IP regarding the identity of the local mobility agent. This tends to eliminate the need for MIP movement detection as well as agent discovery and leads to accelerated Mobile IP hand-offs. It is considered the fastest of traditional Mobile IP movement detection methods.

A very interesting work on the general IP mobility subject is the handoff scheme presented in [21] (*Daedalus* Project): It makes use of *multicasting* and *buffering* mechanisms to reduce the IP handoff latency and obliterate data loss during handoffs. However, it is based on the anticipation of an impeding handoff, and assumes that the handoff is triggered by the mobile client's software. An enhancement of this method is proposed in [4], with the use of a *Domain Foreign Agent* (*DFA*) responsible for multicasting information across multiple cells. A different method is the fast handoff scheme called *Neighbor Casting* [5], which tries to reduce the Mobile IP protocol traffic exchanged over the wireless network during handoffs. For this reason, it provides the APs (mobility agents) with a neighbors map. Unfortunately, it is also based on link-layer triggers for a forecasted handoff. A more recent work on the subject presented in [22], makes a very interesting proposal that significantly shortens the total Mobile IP handoff latency in cases of *hard* and *forward* 802.11 handoffs. It makes use of a timer-driven software *probing* technique, and a Mobile IP advertisement caching and *replay* proxy. So far, it results in the smallest observed MIP handoff delay during network mobility in 802.11 wireless networks (on the order of 100 ms). In order to support fast and seamless handoffs by reducing the delay and data loss during IP handoffs, [12] proposes the following methods: (a) A *Pre-registration* method, which enables the mobile host to communicate with the new foreign agent in the notification of an upcoming handoff, while still attached to its HA, and (b) a *Post-registration* method, which is based on link-layer triggers for tunnel establishment between the two concerned mobile agents. A similar approach is proposed in [20] using a proactive method in which the foreign agent (FA) assists the mobile node to perform a handoff.

Unlike Mobile IP and its optimization variants, IP-IAPP is fully applicable to the IEEE 802.11 infrastructures, and shows better performance over most mobility approaches. Most of the MIP optimization techniques (Table 1) are L2 independent and are based on forecasts of impeding link-layer handoffs. Unfortunately, in the 802.11 case, by no means can the 802.11 clients or the APs predict an imminent handoff. A method based on L2 handoff prediction is not applicable to infrastructure WLANs where link-layer handoffs are *hard* (a wireless station can communicate with only one AP during handover) and *forward* (the station can communicate only with its new AP during the handover). These characteristics introduce limitations to most of the related IP mobility proposals in terms of their applicability and effectiveness on 802.11 wireless networks, as they are expedient only to *soft* (the station is able to communicate with *both* the old and the new AP) and *backward* handoffs. IP-IAPP, however, is not based on forecasts of imminent link-layer handoffs; it gets triggered only on the event of a real L2 handoff. This is why it is forms an appropriate solution for IP handoff support in 802.11 WLANs.

3. The IP-IAPP approach

This IP-IAPP fast IP handoff method complements the 802.11f IAPP to support inter-network movements. It makes use and slightly extends the existing IAPP protocol for HA-FA communication, while no extra wireless traffic is introduced for IP handoff support reasons. The routing methods used by IP-IAPP resemble the well known Mobile IP routing mechanisms; however, IP-IAPP is not an additional network layer protocol, neither does it require support by both APs and 802.11 clients. The movement detection mechanism of the IP-IAPP method is only based on IP-related information integrated into the 802.11 frames. This negates any need for additional protocol traffic exchange between the involved parties (clients and corresponding Access Points (APs) participating in a subnet handoff) **after** completion of the link-layer handoff. In the MIP based approaches however, the MIP protocol signalling of the the Mobile IP agent discovery/solicitation phase (movement detection) poses additional delays to the handoff procedure; the Mobile IP variants are based on Mobility Agent Advertisements to carry out the Movement Detection phase prior to an advanced routing setup necessary for serving the mobile nodes at foreign locations. In the IP-IAPP approach, no additional delays are imposed, as the advanced routing setup at the involved parties is established within a very short interval after an L2 trigger indicating a network handover. All these IP-IAPP key features lead to extremely

Table 1 Summarized comparison table of relevant IP mobility solutions

IP mobility method	Mobile IP compliant	Based on Layer2 handoff prediction	Wireless mode	Handoff latency
Daedalus	No	Yes	Soft	8–15 ms
Domain Foreign Agent	No	Yes	Soft	∼10 ms
Neighbour Casting	Modified MIP	Yes	Soft	NA
Pre/Post Registration	Modified MIP	Yes	Soft	NA
Lazy Cell Switching	Modified MIP	Yes	Soft	>1 sec
Eager Cell Switching	Modified MIP	Yes	Soft	>500 ms
Fast Hinted Cell Switching	Modified MIP	Yes	Soft	<500 ms
Probing & Replaying	Yes	No	Hard	<100 ms
IP-IAPP	No (802.11f compliant)	No	Hard	<50 ms

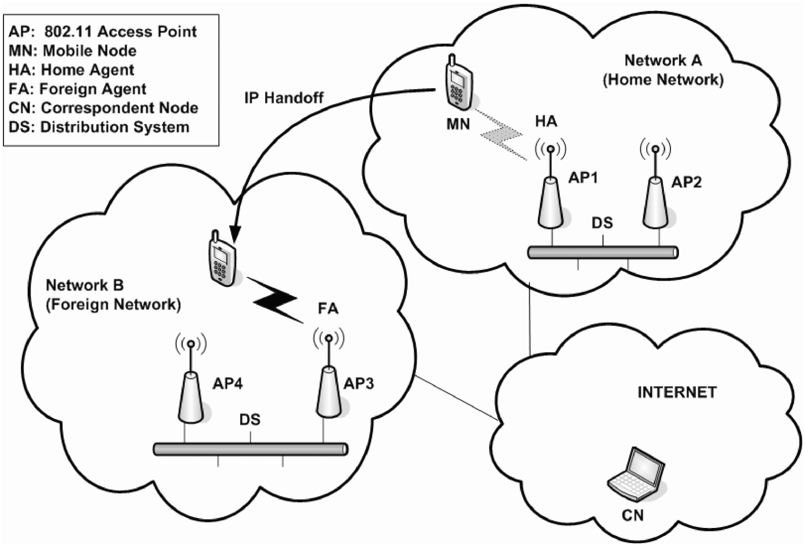


Fig. 1 Entities of the IP-IAPP framework

small IP-reconnection delays of <50 ms and very low packet loss, even without the use of any buffering mechanisms (a future consideration). The total service interruption delay, during which a client cannot receive IP packets, is minimized to the link-layer handoff latency plus one TCP/IP round-trip time. It outperforms existing methods' handoff performance, as it accelerates the total IP handoff procedure. Therefore, the proposed solution effectively combines simplicity with desirable performance.

3.1. IP-IAPP operation basics

The IP-IAPP mechanism is built on top of IEEE 802.11f IAPP. Two new handoff procedures are added to the existing IAPP protocol operation, which handle the IP movements of the clients and offer L3 roaming capabilities. In order for the APs to participate in the proposed L3 roaming protocol, they must support the IP-IAPP core mechanism. This mechanism acts upon link-layer handoffs, and performs a specific IP configuration procedure to support a client's network handoff. It considers APs which serve as mobility agents; the APs are responsible for management and provision of IP mobility support to their associated clients. The MNs preserve their initial home IP address everywhere, regardless of their physical location.

Every MN is assigned a Home Agent inside its home network (HN) Fig. 1. The HA handles mobility of its associated clients, and supports routing of their data even when the clients have roamed to different subnets. The HA is incorporated in the 802.11 AP entity and is also referred to as the Home AP (HAP) of the MN. The HA is the AP to which a station is last associated inside the HN. Every AP acting as a HAP preserves a list of its registered MNs, with all necessary IP mobility related information. When a client moves to a different IP segment, it is associated with a Foreign Agent: the client reassociates with an AP which resides on the foreign subnet. This AP becomes the FA of the MN. The FA is the entity which provides advanced routing services to every associated foreign MN; it is responsible for offering IP connectivity to clients coming from different subnets. The FA is also incorporated in the 802.11 AP entity and is referred to as the Foreign AP (FAP) of the 802.11 MN. Every AP serving as a FAP preserves a list, "Visitor List", of its associated MNs who have roamed from a foreign subnet.

Upon receipt of a L2 trigger by the reassociating (foreign) mobile node, the new AP (FAP) carries out the IP-IAPP *movement detection* phase. In case it figures a network handover during reassociation, it initiates the *IP-IAPP mobility management procedure* instead of the standard 802.11f IAPP. The two involved APs (the FAP and the HAP) carry out a fast notify/response transaction comprising of two TCP/IP IP-IAPP packets (802.11f formatted), and setup a specific framework necessary for routing MN traffic. After successful completion of the IP-IAPP mechanism, the client enjoys IP-connectivity for as long as it remains inside the FN. At its foreign location, the MN is now identified via the foreign AP IP address; this is the Foreign Agent Care of Address (FACOA).

The new IAPP-based packets used in the IP-IAPP handover scheme are TCP/IP packets, exchanged between the involved parties in case of a L3 handover. These packets follow the 802.11f packet format, and are extended to carry the mobility specific information concerning the IP-state of the wireless station. The four new packets and their usage are listed below:

- ***Roam-Request*** [TCP/IP, FAP → HAP]: Causes registration of the FACOA to the HAP, and triggers HAP-FAP advanced routing setup. Follows the IAPP *MOVE-notify* packet format, extended with IP-related context.

- ***Roam-Response*** [TCP/IP, HAP → FAP]: Response to a *Roam-request* packet; informs the FAP about completion of HAP actions (advanced routing setup). Similar to the IAPP *MOVE-response* packet format.
- ***RouteUpdate-Request*** [TCP/IP, HAP → PAP]: Informs the Previous FAP (PAP) for a new movement and causes the removal of stale routing entries at the PAP in cases of intra/inter-foreign network movements.
- ***RouteUpdate-Response*** [TCP/IP,PAP → HAP]: Response to a *RouteUpdate-request* packet, indicating completion of PAP actions (removal of advanced routing setup).

The overall IP mobility management procedure is transparent to the client itself, as it does not participate in any of the IP-IAPP protocol traffic transactions.

3.1.1. Movement detection and location update mechanisms

More specifically, a new Information Element (IE) is added to the 802.11 (Re)Association.Request and Response messages for IP-IAPP purposes. The *movement detection* phase is accomplished via certain MN IP specific information which is acquired from the IP-IAPP IE of the 802.11 Reassociation frames. The MNs are only responsible for filling in this IE with information previously retrieved from the last (Re)Association.Response message; it does not need to perform any decision making upon filling up the IP-IAPP IE. The IP movement detection is every time carried out simultaneously to the L2 reassociation. Therefore, IP-IAPP has zero-delay movement detection phase. The new AP, upon receipt of the Reassociation.Request frame, examines the IP-IAPP IE to identify the current handover case:

(a) If the MN has just performed an intra-network movement, then this involves only a L2 handover (standard IAPP protocol is then initiated by the new AP).
(b) If the MN has just performed an inter-network movement between the Home and a Foreign Network, this is called a *Network HandOver* (NHO): movement from HA to a FA.
(c) If the MN has performed a movement between two FAs of the same (or different) Foreign Network(s), this is a *Foreign NHO* (FNHO).

The NHO and FNHO procedures of the IP-IAPP mechanism which handle the cases of L3 handover are described in the following:

A. The "NHO" procedure:
In this case, the MN reassociates to a New foreign AP (NAP) in a foreign network, while previously associated to its HAP (inside HN). Upon receipt of a Reassociate.Request indicating a NHO handover, the NAP communicates with the HAP, and they establish an advanced routing setup to provide IP-connectivity to the MN at its foreign location. The protocol sequence involved in an *inter-network handover* (NHO) is shown in Fig. 2. The FAP first identifies the handover type. In the event of a NHO, it inserts a mapping for the MN and its HAP to the "Visitors List". It quickly informs

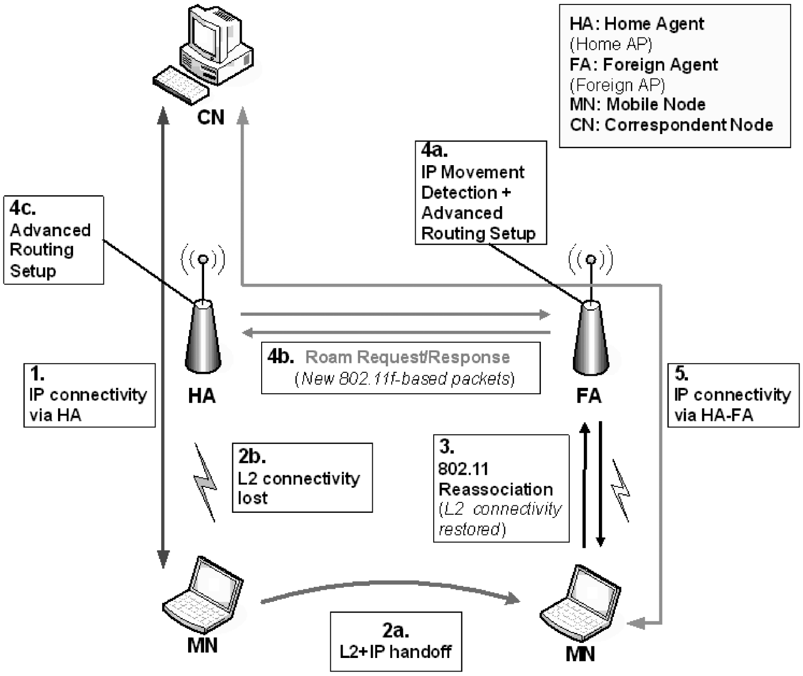


Fig. 2 Phases of the IP-IAPP NHO procedure

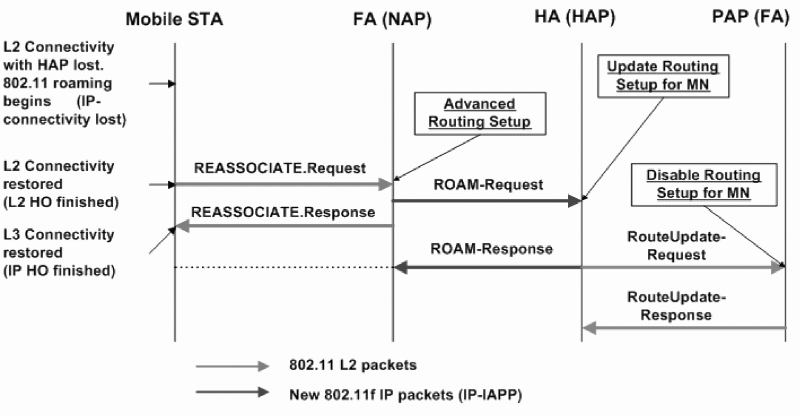

Mobile STA
FA (NAP)
HA (HAP)
PAP (FA)
L2 Connectivity with HAP lost. 802.11 roaming begins (IP-connectivity lost)
L2 Connectivity restored (L2 HO finished)
L3 Connectivity restored (IP HO finished)
Advanced Routing Setup
Update Routing Setup for MN
Disable Routing Setup for MN
REASSOCIATE.Request
ROAM-Request
REASSOCIATE.Response
ROAM-Response
RouteUpdate-Request
RouteUpdate-Response
802.11 L2 packets
New 802.11f IP packets (IP-IAPP)

Fig. 3 Phases of the IP-IAPP FNHO procedure

the HA of the MN about this event via transmission of a Roam-Request message with a type of NHO. The FAP is responsible for capturing all IP traffic destined to the MN, and for forwarding all IP traffic originating at the MN to its Home Agent through the established IP-IP tunnel. The HA, upon receipt of a Roam-Request message, updates its MN association list to indicate that the specific MN is currently "away" from HN. It also maps the MN IP address to the FAP IP address (FACOA). The HAP intercepts all IP traffic which arrives in the Home Network and is destined to the MN IP address, and then routes these packets towards the MN current FACOA.

After completion of the IP-IAPP inter-AP communication, the mobile client regains IP connectivity via the IP-IP tunneling routing methods. The MN is again able to transmit/receive packets using its original IP address, while connected to the FA. As soon as the client restores network connectivity, there follows an intermediate adjustment period until its previously ongoing sessions are fully restored. This is the time until the client (IP host) retrieves information related to the remote end of sessions initiated at the HA (e.g. update its ARP table), so packets are now routed through the FA-HA tunnel. The client can continue communicating with the correspondent hosts only after this short time period. This procedure may take non negligible time to complete, because the client is not aware of the instant when network connectivity is lost or restored. As a result of this, the client does take immediate action after IP connectivity restoration. The IP-IAPP mobility entity in the FA takes action so as to assist the client in restoring the previous sessions as soon as possible. More specifically, the FA triggers ARP cache update by the client, and in so doing reduces packet loss during handover as it shortens the restoration time for any active sessions.

B. The "FNHO" procedure:

The MN reassociates to a new foreign AP, while previously associated to another foreign AP. Upon reassociation, the new foreign AP identifies a FNHO handover. The protocol procedure consists of the same phases as in the inter-network movement, with an addition of a communication between the HA and the previous foreign agent. Both APs delete the previous routing setup concerning this MN (Fig. 3).

The FAP inserts a mapping for the MN and its HAP to its "Visitor List", as in the NHO case. It quickly informs the MN HA of this event via transmission of a Roam-Request message with a type of FNHO. This type of Roam-Request also carries information about the previous FAP. The new foreign agent immediately sets up an IP-IP tunnel towards the HA IP address, and performs the same advanced network setup as in the case of a NHO. The HA, upon receipt of a Roam-Request message indicating a FNHO, updates its MN association list: it maps the MN IP address to the new FAP IP address, and characterizes the previous FAP as "TEMP". As for the advanced routing, it firstly creates an IP-IP tunnel towards the new FAP, and adds the same routing entries as in the case of a NHO, however the new rules refer to the new FAP IP address. As soon as the setup for the new MN location is successfully established, it sends a RouteUpdate-Request to the previous FA, and disables all routing entries which referred to that tunnel. In the case of a FNHO, any IP datagrams intercepted by the HAP, after the new registration, are delivered to the MN new location (FACOA). It is possible that some packet may escape through the existing tunnel towards the previous FA, until the HA routing setup is appropriately updated. The previous tunnel is disabled and deleted within a few milliseconds, and all the packets are properly routed via the new active tunnel between the HA and the new FA. After completion of the FNHO IP-IAPP procedure, the routing of MN IP traffic is handled the same way as in the NHO case. Again, the total IP service interruption is short enough to successfully restore the ongoing sessions during a FNHO.

3.1.2. Fault tolerance

An IP-Binding Liveliness (IPL) mechanism is also added to the IP-IAPP entity, which assists in fault tolerance, resource conservation, and improved management of active sessions. Every Home AP and Foreign AP who has established tunnels towards peer APs (serving L3 roaming enabled stations) make use of the IPL mechanism in order to monitor the status of the established sessions, the status of the remote end (remote AP), and the connectivity status of the served mobile node. This functionality is necessary in cases of unexpected disassociation of MNs or other miscellaneous events, like sudden shutdown of the peer AP, which could potentially cause disturbance of the proper operation of the IP mobility support service. Examples of such cases are: (1) Renewal of MN IP while in FN, (2) Reboot of current FA, (3) Bad status of HA-FA network link while having an active tunnel, (4) Sudden disassociation of an MN (shutdown, weak wireless link, or other reasons) while in FN (active HA-FA tunnel). The IPL mechanism comprises of certain messages that are periodically exchanged between HAs and FAs which have established an IP-IP tunnel and serve MNs that have currently roamed to foreign networks. It is incorporated in IP-IAPP for monitoring and fault-tolerance reasons, and ensures the normal operation of the method as well as the network connectivity of the roaming clients. In the event of a faulty situation, the tunnels related to the corresponding MNs are deleted, all related advanced routing setup is disabled, and in most cases the involved AP triggers an MN disassociation. In this case, the IP and 802.11 state of the MN needs to be resettled in order to to regain IP connectivity.

3.2. Enhancements for advanced services

3.2.1. Support of Inter-AP authentication

Extending the 802.11f proposal, the RADIUS server is used in the IP-IAPP mechanism to provide inter-AP authentication and secure communication of APs which belong to different distribution systems (IP subnets). This provides the IP-IAPP interactions with a level of security and excludes movements to rogue FAs. In the IP-IAPP framework, we consider a set of subnets which form an *IP-mobility enabled WLAN domain (IPMOD*). The RADIUS server provides registration and authentication services to every AP of this set. Analogously to the IAPP procedure, upon power up, every IP-IAPP enabled AP registers itself to the RADIUS server as a valid *IPMOD* member. Next, it retrieves a "*candidate FA list report*" from the RADIUS server. This report contains information on APs which run on the same *IPMOD* and are *valid* candidates for a mobile IP host. All APs participating in this domain must be IP-IAPP enabled, i.e. they must provide IP mobility support to their registered clients. This is advertised to the RADIUS server of the *IPMOD* during the registration phase. Upon reassociation of a foreign client, the FA searches its local cache to check the validity of the station's HA. If the HA is a registered member of *IPMOD*, then the IP mobility services are available for this station. Otherwise, the FA queries the *IPMOD* RADIUS server. The IP handoff is supported only if a client's subnet roaming is towards valid IP-IAPP enabled APs. A foreign agent will not launch a communication towards a non-authenticated HA (not an IPMOD member). Thus, the interactions which take place during the IP handoff IP-IAPP procedure between foreign APs are secure, and may also be encrypted (optional, as in 802.11f IAPP).

3.2.2. Zero requirements by the 802.11 clients

As previously stated, the IP-IAPP makes the mobility support procedure invisible to the clients, while requires no additions in their protocol stack. In the initial proposal, the IP roaming enabled clients needed only to integrate a minor add-on to their existing 802.11b software implementation (location specific information transfer). This extension served for the APs to perform the necessary movement detection and recognize an IP handoff in case of subnet movements. In order to eliminate even the smallest involvement of the stations, the small addition in the stations' software has been omitted. Every 802.11 client can now be served by the IP-IAPP mobility feature of the APs, without any IP-IAPP patching. We now use a combination of centralized and distributed caching of the necessary IP location specific data. The RADIUS server is used for centralized caching of the necessary information. Every AP of this subset which serves as an HA for a number of stations, provides the RADIUS server with a user's IP-IAPP related information for every newly associated station (centralized caching). At the same time, this information is broadcasted to the rest APs which are members of the *IPMOD* (distributed caching). If a roaming station is not originating from an AP which belongs to the set of valid subnets, or if there is no IP configuration data in the RADIUS registry, then it is handled as a newly associated station, using the standard IAPP association procedure. The FA does not trigger the mobility support service and does not utilize any advance IP routing for this client; the client must obtain a valid IP address inside the new subnet in order to gain network layer connectivity after successful reassociation. The RADIUS server assists in the consistency of remote APs' cache, and is used as an alternative in cases of failures. It's role is to coordinate and help all APs to serve the IP-IAPP enabled devices in a safe and correct manner, without the need of clients' involvement.

3.2.3. Support of both static and dynamic IPs

The initial IP-IAPP proposal offers advanced mobility services to wireless IP hosts which use a *static* IP address. While attached to a foreign AP, the users enjoy IP connectivity via their original network layer address (matching their home subnet span), as long as this address is not invalidated. In the new enhanced proposal, the IP-IAPP mechanism can also support subnet handoffs for users who use *dynamic* IP address. These stations obtain a valid network address inside the Home Network via DHCP. After certain period of time, the networking module of the client may perform address renewal. The IP-IAPP module running on 802.11 APs handles the address changes/renewals for users with dynamic IP. In all cases, the protocol preserves consistency in the network state information which is cached at each member of the IPMOD, while achieves to preserve IP connectivity of currently roaming clients via their home network. More specifically:

(a) While in HN, if a client performs a DHCP address renewal, the new address will most likely be identical to its initially assigned one. No action needs then to take place by the HA.

(b) While in HN, if the client is assigned a different IP address after a DHCP request, this address will again match its home subnet span. In this case, the HA notifies the *IPMOD* APs and the RADIUS server about this address change. The RADIUS server and the APs update their cache with the new IP-specific information. Therefore, they still can handle possible future network handoffs, by being in sync with the latest IP state information of all clients.

(c) While attached to a FA, a mobile user sends and receives IP traffic using its home IP address, with the help of certain IP routing setup at its foreign and home agent. If the station transmits a DHCP request, then this packet is forwarded to the home DHCP server, as all IP data passes through the home agent after the IP-IAPP routing setup. Therefore, again the new address will match the home subnet span, and the same actions take place as in case (b). From now on, the home and the foreign agents are able to route the “new” IP host’s datagrams.

(d) If a client who is currently served by the mobility methods of IP-IAPP, while connected to a foreign agent, by some means obtains an IP which no longer match its home network, then the FA becomes its new HA, and disables previous advanced routing setup for the client. The previous HA is informed about the topological change of its registered client, and ceases any previous HA-specific mobility services for this station.

4. Performance measurements and results

4.1. Test environment

The testbed used in the performance testing of the proposed fast IP handoff method is shown in Fig. 4. The IP mobility entity has been implemented on the wireless router/Access Points based on Atmel’s AT76C*511* (IEEE 802.11) with 802.11f IAPP support, with wired interface configured at 100 Mbps and wireless interface configured at 11 Mbps. The mobile clients are a laptop computer (Pentium IV) with 802.11

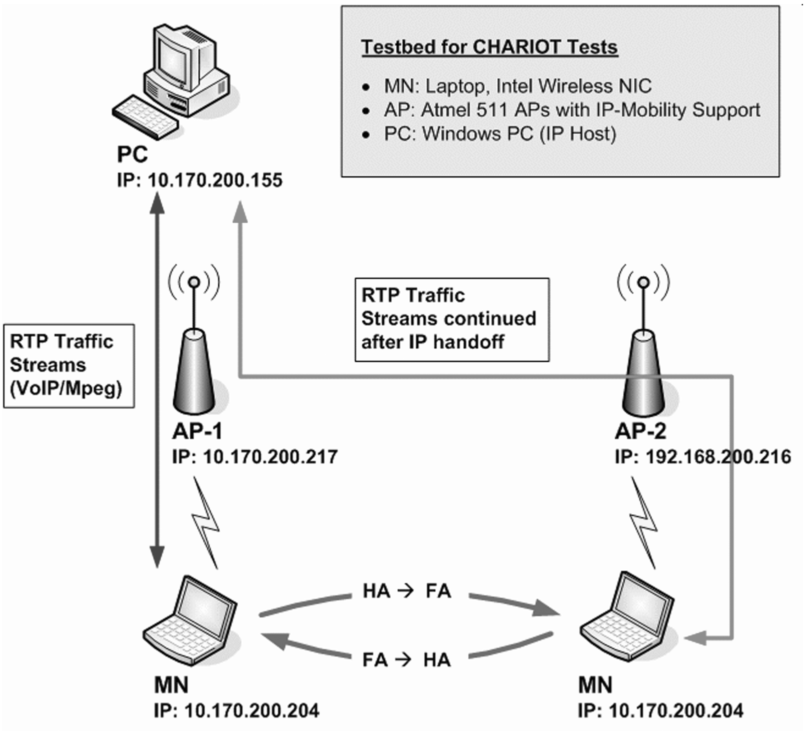

Testbed for CHARIOT Tests
• MN: Laptop, Intel Wireless NIC
• AP: Atmel 511 APs with IP-Mobility Support
• PC: Windows PC (IP Host)
PC
IP: 10.170.200.155
RTP Traffic Streams (VoIP/Mpeg)
RTP Traffic Streams continued after IP handoff
AP-1
IP: 10.170.200.217
AP-2
IP: 192.168.200.216
HA → FA
FA → HA
MN
IP: 10.170.200.204
MN
IP: 10.170.200.204

Fig. 4 Testbed for CHARIOT tests

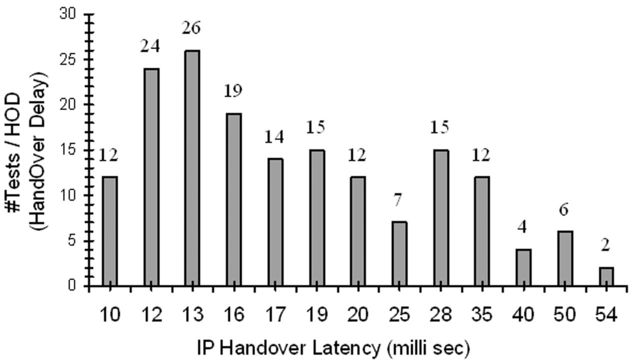


Fig. 5 Cumulative Frequency Density of total handoff period

Intel wireless cards, and 802.11 Atmel VoIP phones. The APs used in the testbed are Atmel 511 APs with IP-IAPP support. The APs are distributed and reside on different IP subnets, which form the IP-IAPP *IPMOD*. The correspondent hosts are desktop PCs running open IP sessions with the mobile clients.

4.2. Results from ICMP (Ping) sessions

The clients were running ICMP sessions and roamed between the three subnets. The performance metrics during the ICMP tests were: (a) the total IP handoff latency (link-layer plus network-layer handoff delay) until restoration of the ongoing sessions, and (b) the packet loss. The laptop, while attached to its home agent, launches an ICMP session towards a remote IP host. During this open session, it roams to an AP of an adjacent foreign subnet (IP handoff). The total IP handoff latency is measured as the delay between the time that the last ICMP packet was received by the client (while wirelessly connected to its HA), until the first packet received through the FA. The histogram of the handoff latency measurements is shown in Fig. 5.

What is observed is a very small *total* handover latency (802.11 handoff delay plus IP connectivity restoration period). The mobile client regains connectivity after a maximum of 54 msec (worst case), and 13 msec in the best case. Classical MIP has handover latency $>$ 1 sec, while all the MIP optimization mechanisms have shown total handover latency $>$ 300 msec. The variation in handover latency values is due to the backbone traffic (Ethernet & wireless LAN). All tests were performed under normal (real) networking conditions, e.g. other traffic existed both over the air and over the Ethernet medium. As shown in Fig. 6, the maximum number of packet loss is 9 packets (ping session with 1 msec interval). The minimum is 2 packets. The results verify that the packet loss is very small. The amount of packets which appears in the graphs includes those IP packets that reached the station right after the handover (IP connectivity already restored), but were not *answered* by the client. These packets successfully reached the roaming client but could not be replied, due to the transitional delay until a mobile host updates its ARP table after having moved to a foreign subnet; not due to the IP connectivity gap caused during the handover.

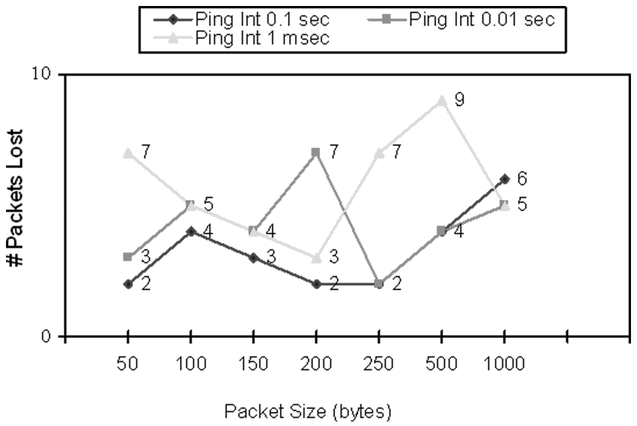


Fig. 6 Packet Loss vs packet size

4.3. Tests with real time & multimedia traffic

The *Chariot* Console [18], was used to measure the handoff performance under real-time and multimedia traffic. One NetIQ Performance Endpoint was used at the wireless client (laptop), and another one at the correspondent IP host (PC). In all tests, the laptop performed subnet roaming while having an active IP session towards the correspondent IP host. The measurements were retrieved for movements from the HA to the FA and vise versa (NHO). We also examined the scenario for client movements between two FAs (FNHO). In this test case, the client was attached to the AP-2 and roamed to another AP (not its HA) of a different subnet (10.170.254.0).

In the first test (Fig. 7), the client was running a VoIP session towards the PC (RTP Stream, Chariot *G.711u* script). The client roams from HA to FA at around 17th second of the Chariot test, and from FA back to HA at around the 24th sec. What can be observed are the very small one-way delay of 3 msec (this is the network delay; latency as the difference between the time a datagram is sent by the source endpoint and the time it was received by the destination endpoint) and an acceptable packet loss ($\sim$=11 consecutive datagrams lost during the NHO).

The overall throughput suffered a degradation of only $\approx$9%. To determine the quality of VoIP under packet loss, the most common metric is the Mean Opinion Score (MOS) [9], which evaluates the effect of bursty loss on VoIP perceived quality (the Overall Voice Quality). In a MOS test, the listeners rate audio clips by a score from 5 to 1, with 5 meaning Excellent, 4 Good, 3 Fair, 2 Poor, and 1 Bad. The MOS estimate of the first Chariot test shows that the call was not interrupted; It only suffered substantial quality

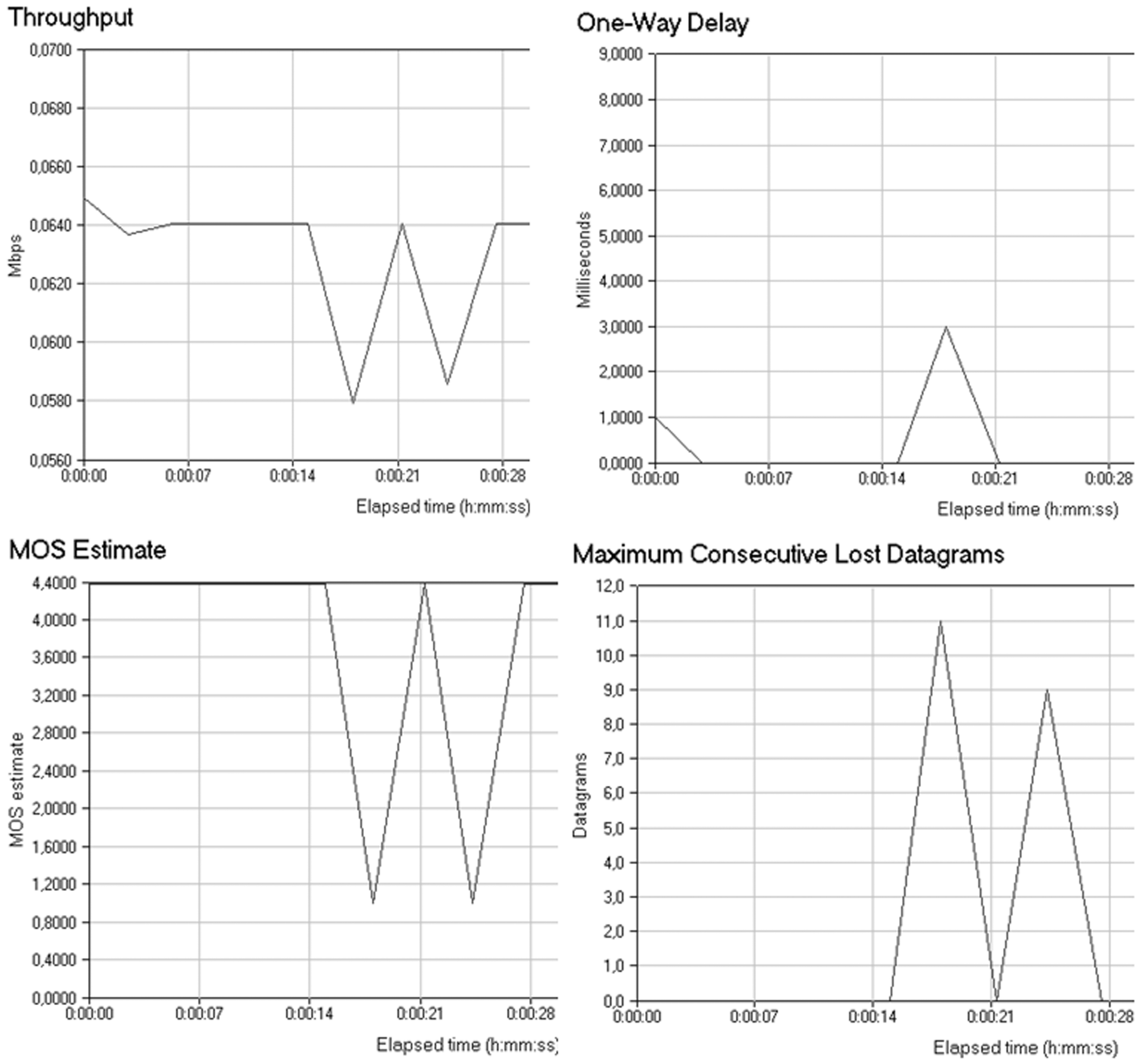


Fig. 7 Test 1: VoIP session (RTP Stream) – Movements between HA-FA

degradation with a low peak at MOS = 1, and quickly restored its initial quality: MOS = 4.4 (Chariot *G.711u* script represents a VoIP call using a newer version of the G.711 codec, which uses a larger packet size: Data Rate = 64 kbps, Buffer Size = 160 bytes, MaximumMOS = 4.4).

In the second test using again a VoIP session, the client roams from an FA to a new FA approximately at the 16th second, and from the new FA back to the HA at around the 37th sec. As can be seen from Fig. 8, all results are increased by a small factor. During the FNHO, the session throughput suffered a degradation of about 19%, and the one-way delay in now almost 27 msec. This is due to the fact that the HA must first disable all previous IP settings for forwarding packets to the previous FA (remove tunnels, explicit route entries, proxy ARP entries, etc). This poses a small additional delay to the overall IP reconnection period. Again the IP handoff delay is small enough to efficiently preserve the VoIP session, as also verified by the MOS estimate.

The third test measured the performance of IP-IAPP for multimedia traffic (Fig. 9). The client roams from HA to an FA, running an open Cisco IP/TV:MPEG Audio Stream session (Chariot *IPTVa.sc* script represents a Cisco System's IP/TV application, MPEG audio or video streams: Data Rate = 93 kbps, Buffer Size = 1278 bytes) towards

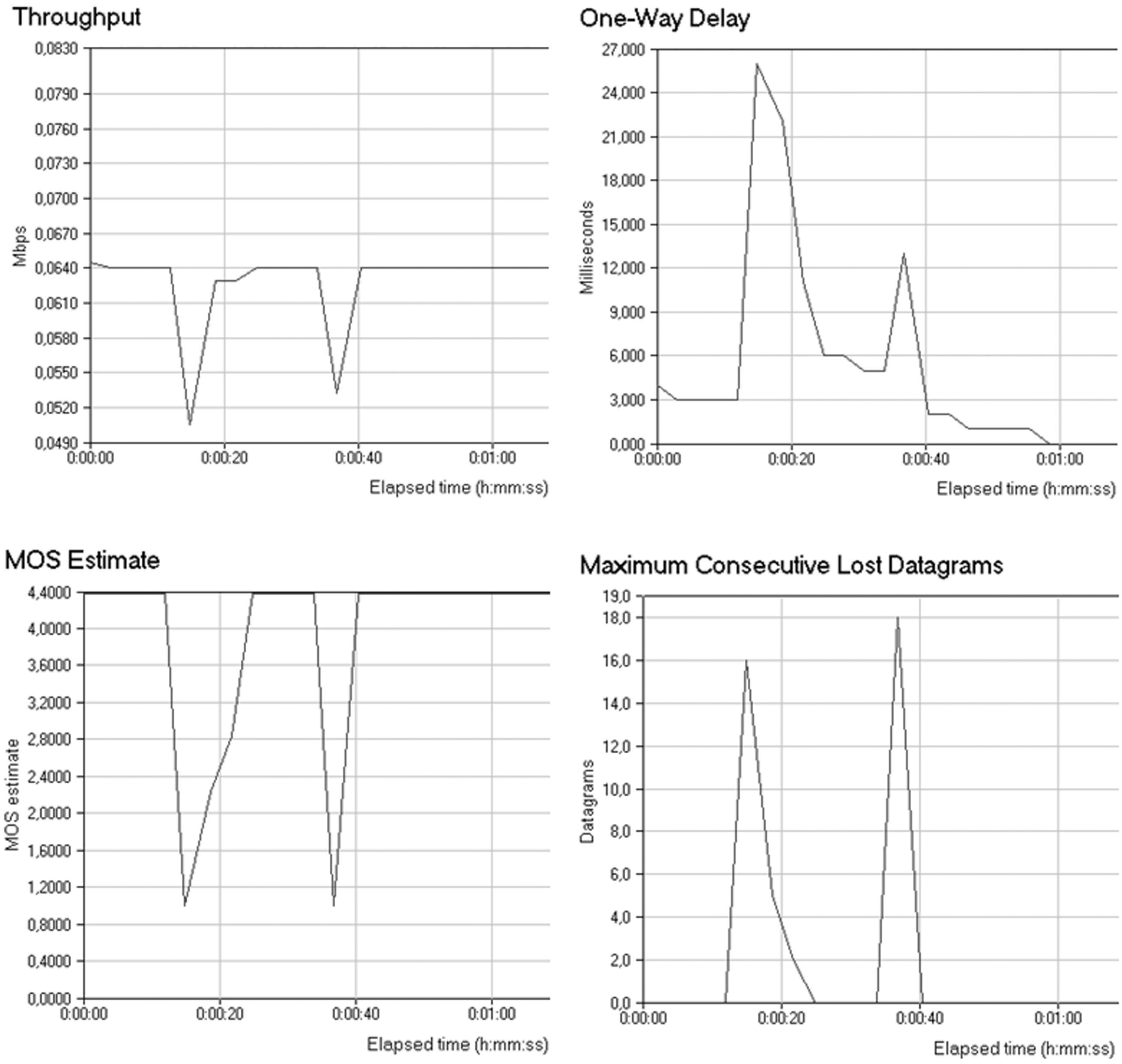


Fig. 8 Test 2: VoIP Session (RTP Stream) – Movements between two FAs

a correspondent IP host. The client roams forward approximately at the16th sec of the Chariot test, and from the FA back to the HA at around the 32nd sec. The throughput degradation is about 18%, while handoff delay (53 msec) is increased compared to the previous tests (VOIP sessions). This is due to the different traffic characteristics of the two applications (IP/TV application has larger buffer size and larger packet size at a highest data rate). However, the handoff latency is again very small and the connection is quickly restored. The results shown in Fig. 9 verify that IP-IAPP both preserves and rapidly restores IP connectivity, even for clients running real-time multimedia applications.

Lost data can mean lost scenes in a video application. Likewise for telephone calls: lost data can cause the speaker's voice to sound unintelligible. The amount of accepteble data loss varies by application; some real-time applications can tolerate certain amounts of lost data because they buffer data as it is received. Other applications don't tolerate lost data. As verified by real experimental results, the IP-IAPP method significantly contributes in shortening the total IP handoff latency during subnet movements. As a result, the demanding real time and multimedia applications suffered very small quality degradation in all cases and were quickly restored.

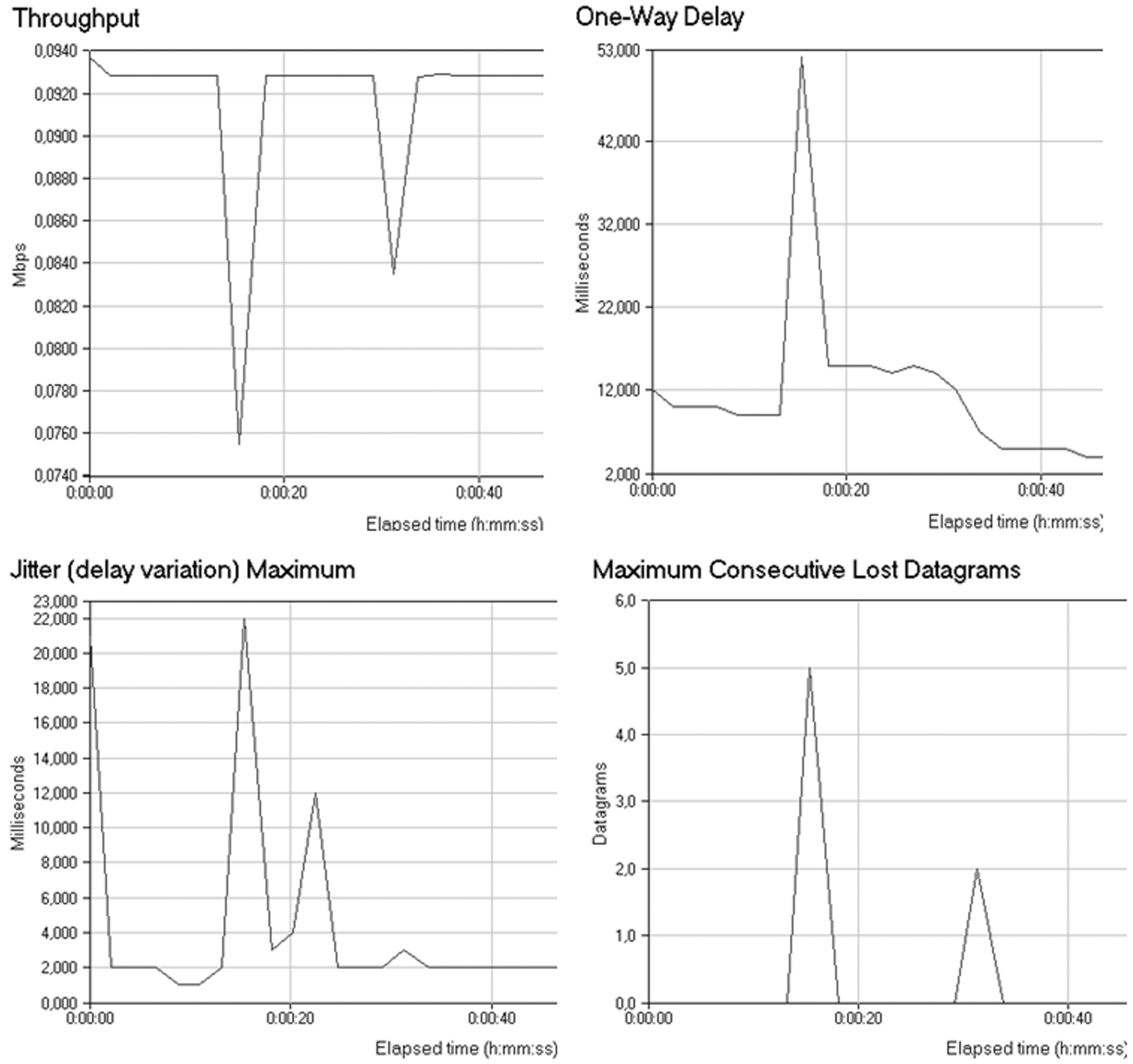


Fig. 9 Test 3: IP/TV Video (Mpeg) session

5. Conclusions and future work

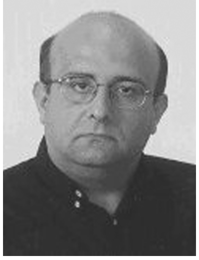
Research in IP mobility support and handoff optimization is driven by the need to support next generation applications running upon wireless links. Real-time and demanding applications such as VoIP calls should be preserved even in the event of a subnet roaming. At the same time, the experienced performance degradation must be insignificant and not even noticeable to the client. The IP-IAPP IP handoff method supports both the above requirements. The mobile hosts utilizing VoIP and other multimedia applications are freely moving around between neighboring subnets, using their home address, without experiencing any service interruption and without even realizing the IP handoff. It works on the existing 802.11 framework, adds no extra protocol traffic, and is applied only to the APs. However, it still achieves seamless and smooth handoffs, without aggravating the 802.11 clients, unlike existing proposed IP mobility solutions.

Currently, no buffering is implemented at the APs. Using a buffering technique to the HAs for client's incoming packets (very small buffer size needed, as shown from all the test results), there could be even zero packet loss via our proposed method. Next tests will be focused on measurements using advanced buffering mechanism on the APs for the IP roaming-enabled stations. Another future consideration is to incorporate the use of IPv6 tunneling when needed, e.g. in WLAN systems where the Distribution System (DS) built on IPv6 technology. A very important issue is to study ways to extend the current IAPP-based RADIUS protocol usage to support fast and secure transfer of station's context (such as QoS parameters [19], IPsec, etc.), as well as to support *roaming-specific services* in 802.11 WLANs [10, 11]. At its current version, the IP-IAPP method may can be applied in small and medium sized WLAN systems comprising of a small number of different IP subnets, where the mobile clients do not travel very far from their Home Network (small number of intermediate routers). It is not yet to be deployed in large scale WLAN configurations. A next step is also to make appropriate modifications so as to support large scale systems, e.g. deployment by an ISP. Finally, the predominant subject of our future work is to examine possible ways to combine the IP-IAPP method, which supports fast inter-subnet handoffs, with the emerging 802.11r protocol [13], which studies ways to support fast inter-BSS transitions in general, with QoS and Security considerations.

References

1. 802.11F^{TM}, IEEE Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11^{TM} Operation.
2. C. Perkins, ed., *IP Mobility Support*, RFC 2002 (Oct. 1996).
3. C.E. Perkins, *Mobile IP, Design Principles and Practices*, Wireless Communications Series, Addison-Wesley (1997).
4. C. Tan, S. Pink and K. Lye, A Fast Handoff Scheme for Wireless Networks, Second ACM International Workshop on Wireless Mobile Multimedia (1999).
5. E. Shim and R. Gitlin, *Neighbor Casting: A Fast Handoff mechanism in Wireless IP Using Neighbouring Foreign Agent Information*, New York Metro Area Networking Workshop (2001).
6. H. Petander, *Mobile IP Route Optimization*, White Paper, Helsinki University of Technology (May 2000).
7. IEEE, IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Institute of Electrical and Electronics Engineers, (Nov. 1999).
8. I. Samprakou, C. Bouras and T. Karoubalis, *Fast and Efficient IP Handover in IEEE 802.11 Wireless LANs*, 2004 International Conference on Wireless Networks (ICWN'04), Las Vegas, Nevada, USA, (June 2004).
9. International Telecommunication Union, *Subjective Performance Assessment of Telephone-Band and Wideband Digital Codecs*, Recommendation P.830, Telecommunication Standardization Sector of ITU, Geneva, Switzerland, (Feb. 1996).
10. J. Caron, *Public Wireless LAN Roaming Issues*, Draft-Caron-Public-WLAN-Roaming-Issues-00.txt (Feb. 2002).
11. J. Loughney, M. Nakhjiri, C. Perkins and R. Koodli, *Context Transfer Protocol*, Draft-ietf-seamoby-ctp-08.txt, (Jan. 21, 2004).
12. K. Malki, P. Calhoun, T. Hiller, J. Kempf, P. McCann, A. Singh, H. Soliman, and S. Thalanany, *Low Latency Handoffs in Mobile IPv4*, Internet Draft, Mobile IP Working Group (Jun. 2002).
13. M. Montemurro and D. Engwer, *Roaming Requirements Discussion*, Doc.: IEEE 802.11-04/286r0 (March 2004).
14. N.A. Fikouras, A.J. Konsgen and C. Gorg, *Accelerating Mobile IP Hand-offs Through Link-Layer Information*, International Multi-conference on Measurement, Modelling, and Evaluation of Computer-Communication Systems (MMB), Aachen, Germany (Sept. 2001).
15. N.A. Fikouras and C. Gorg, *Performance Comparison of Hinted and Advertisement Based Movement Detection Methods for Mobile IP Hand-offs*, Elsevier Science, Computer Networks, 37(1), 55–62, (2001).
16. N.A. Fikouras and C. Gorg, *A Complete Comparison of Algorithms for Mobile IP Hand-offs with Complex Movement Patterns and Internet Audio*, 4th International Symposium on Wireless Personal Multimedia Communications (WPMC), Aalborg, Denmark (Sept. 2001).
17. N.A. Fikouras, K. El Malki and S.R. Cvetkovic, *Performance Analysis of Mobile IP Handoffs*, Asia Pacific Microwave Conference 1999 (APMC), Singapore (December 1999).
18. NetIQ Chariot Console, http://www.netiq.com/products/chr/default.asp.
19. N. Passas and L. Merakos, *Unified QoS Provision in Wireless Access Networks*, Wireless, Mobile and Always Best Connected, 1st International ANWIRE Workshop, Glasgow, UK (April 22, 2003).
20. P. Calhoun, T. Hiller, J. Kempf, P. McCann, C. Pairla, A. Singh and S. Thalanany, *Foreign Agent Assisted Handoff*, Internet Draft, Draft-ietf-mobileip-proactive-fa-03.txt (Nov. 2000).
21. S. Seshan, H. Balakrishnan and R. Katz, *Handoffs in Cellular Wireless Networks: The Daedalus Implementation and Experience*, Kluwer International Journal on Wireless Communication Systems (1996).
22. S. Sharma, N. Zhu and T. Chiueh, *Low-Latency Mobile IP Handoff for Infrastructure-Mode Wireless LANs*, IEEE Journal on Selected Areas in Communication, Special issue on All IP Wireless Networks (2004).

Ioanna F. Samprakou received her B. Eng in Computer Engineering and Informatics in 2000 and her MSc. in the same area in 2003 from the University of Patras, Greece. She is currently a Ph.D canditate at the University of Patras. She has joined Atmel SA in 2002, where she is a Senior Wireless System Eng at the System Concept and Design group. She specializes in wireless technologies, and mobile communications, and holds a patent in the field of IP mobility. She has led teams in developing wireless 802.11 products such as Wi-Fi APs, STAs, and VoIP phones. Previously she has worked for the Research & Academic Computer & Technology Institute of Patras (RACTI) as an R&D computer engineer. She is a member of the Technical Chamber of Greece.



Christos J. Bouras obtained his Diploma and PhD from the Computer Science and Engineering Department of Patras University (Greece). He is currently an Associate Professor in the above department. Also he is a scientific advisor of Research Unit 6 in Research Academic Computer Technology Institute (CTI), Patras, Greece. His research interests include Analysis of Performance of Networking and Computer Systems, Computer Networks and Protocols, Telematics and New Services, QoS and Pricing for Networks and Services, e – learning, Networked Virtual

Environments and WWW Issues. He has extended professional experience in Design and Analysis of Networks, Protocols, Telematics and New Services. He has published 200 papers in various well-known refereed conferences and journals. He is a co-author of 7 books in Greek. He has been a PC member and referee in various international journals and conferences. He has participated in R&D projects such as RACE, ESPRIT, TELEMATICS, EDUCATIONAL MULTIMEDIA, ISPO, EMPLOYMENT, ADAPT, STRIDE, EUROFORM, IST, GROWTH and others. Also he is member of, experts in the Greek Research and Technology Network (GRNET), Advisory Committee Member to the World Wide Web Consortium (W3C), IEEE Learning Technology Task Force, IEEE Technical Community for Services Computing WG 3.3 Research on Education Applications of Information Technologies and W 6.4 Internet Applications Engineering of IFIP, Task Force for Broadband Access in Greece, ACM, IEEE, EDEN, AACE and New York Academy of Sciences.

Theodore E. Karoubalis. received his B. Eng in Computer Engineering and Informatics in 1992 and his Ph.D. in the same area in 1996 from the University of Patras, Greece. He has joined ATMEL Hellas SA at 1998. Since 1998 he is the Manager of PSLi software dpt. and since 2002 he is the manager of System and Concepts dpt. His interests include systems on chip, embedded applications, wireless systems etc. He is a member of IEEE and the Technical Chamber of Greece.