Terminal Independent Mobility for IP (TIMIP)

António Grilo, Pedro Estrela, Mário Nunes, INESC/IST, PORTUGAL

ABSTRACT

This article presents the Terminal Independent Mobility for IP (TIMIP), which is a new architecture for IP mobility in wireless access networks. TIMIP is based on principles similar to those in the CIP and HAWAII architectures proposed at IETF and equally suited for micromobility scenarios. With TIMIP, terminals with legacy IP stacks have the same degree of mobility as terminals with mobility-aware IP stacks. Nevertheless, it still uses MIP for macromobility scenarios. In order to support seamless handoff, TIMIP uses context-transfer mechanisms compatible with those currently in discussion at the IETF SeaMoby group.

INTRODUCTION

Increasing demand for user mobility throughout the global Internet has launched a successful wireless LAN market and created the need for a new Internet architecture. While layer-2 mobility is easy to accomplish and is already supported in most commercial WLAN cards, it does not allow terminals to roam between different LANs and to cross between router domains. Layer-3 mobility allows Internet-wide mobility at the cost of more complex management. Several reference models for IP micromobility have already been proposed by the IETF, each with different advantages and disadvantages, the main proposals being MIP, HAWAII, and CIP. However, it should be noted that these three proposals require the mobile terminal to be mobility-aware, which requires the replacement of the legacy IP protocol stacks (a hard task if we consider the variety of mobile terminal operating systems and versions). This article presents the specification of Terminal Independent Mobility for IP (TIMIP), which is a new proposal for IP mobility in wireless access networks. Unlike the existent IETF proposals, TIMIP can be totally implemented in the network nodes and work transparently to the IP layer of the terminals. The proposed architecture is depicted in Fig. 1.

A TIMIP domain is an IP subnet organized as a logical tree of access routers whose root is the access network gateway. The latter interfaces with the IP core network, which in turn connects to other access networks. The different elements of the wireless access network have the following roles and capabilities:

- **Access router (AR)**: The access network is formed by a number of routers organized in a logical tree topology. Each router incorporates mobility management functions.
- **Access point (AP)**: The AP is an AR that directly communicates with the mobile terminals at the radio interface. It is designed with the IP functionality of an AR because in this way IP mobility and QoS can be integrated at the radio interface. The AP sends/receives IP packets with application data to/from the mobile terminals. The AP is also responsible for detecting handoff and triggering mobility management procedures on behalf of the mobile terminal.
- **Access network gateway (ANG)**: The ANG is the root AR of the wireless access network, interfacing with the core IP network. The ANG also performs special mobility management functions related to the support of MIP-based macromobility.
- **Mobile terminal (MT)**: The MT runs the user applications. Roaming between different APs is performed by layer-2 in a way that is transparent to the IP layer of the MT.

An overview of the IP Mobility reference models in discussion by the IETF is provided next, followed by the description of TIMIP. The article ends with some conclusions.

IP MOBILITY IN IETF

Of the IP mobility protocols already proposed at the IETF, MIP could be used in both micromobility and macromobility scenarios, though its use for micromobility presents some efficiency problems that can affect IP QoS. For this reason CIP and HAWAII were proposed as means to

0163-6804/01/$10.00 © 2001 IEEE

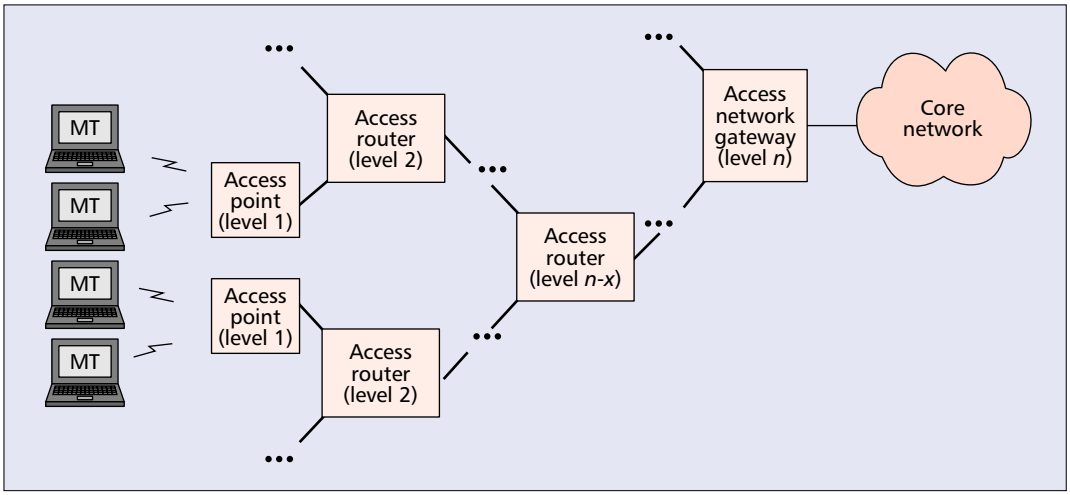

Figure 1. *Architecture of a TIMIP wireless access network.*

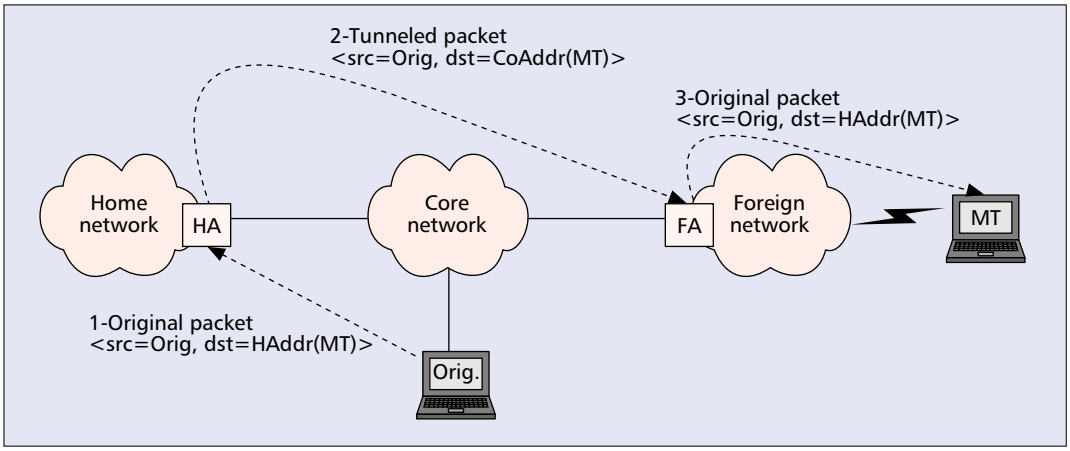

Figure 2. *MIP architecture and message flow.*

optimize micromobility, while they still rely on MIP to implement macromobility.

Mobile IP

The main framework for IP mobility in the IETF is Mobile IP (MIP), specified in RFC 2002 [1]. Its architecture and message flow are depicted in Fig. 2. In the MIP model, a mobile terminal has two addresses: the home address (HAddr) and the care-of address (CoAddr). The HAddr is the address that the terminal retains independent of its location. This address belongs to the home network of the terminal, which is the IP sub-network to which the terminal primarily belongs. The CoAddr is a temporary address assigned to the terminal within a foreign network.

When the mobile terminal is located within its home network, it receives data addressed to the HAddr through the home agent (HA). When the mobile terminal moves to a foreign network, it obtains a CoAddr broadcast by the foreign agent (FA) in **router advertisement** messages as defined in RFC 1256 [2]. This CoAddr is then registered with the HA with a **registration request** message. Whenever a packet arrives at the HA addressed to the HAddr of the mobile terminal, the HA checks if the mobile terminal is currently located on a foreign network. In this case the HA tunnels the packet within an IP packet addressed to the FA. When the FA receives the packet, it de-encapsulates it and forwards it to the mobile terminal. Packets sent by the mobile terminal are routed normally, even if the terminal is located in a foreign network.

As MIP relies on normal routing, it presents several problems, namely the need for triangulation through the HA when the terminal is located on a foreign network. Triangulation and IP tunneling are difficult to integrate with RSVP. Besides, triangulation may cause a significant increase in end-to-end transmission delay, being especially inefficient when the mobile terminal is receiving data originated from the foreign network where it is currently located. This model can be optimized if the originator of the packets is a MIP terminal. In this case the HA sends the originator a **binding update**, containing the CoAddr of the destination. Further packets are sent directly to the CoAddr instead of the HAddr.

HAWAII

The Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [3] was proposed in order to solve the QoS and efficiency issues of MIP. In this model the terminals implement MIP as before, while special forwarding entries are installed on specific routers, making them

As MIP relies on normal routing, it presents several problems, namely the need for triangulation through the HA when the terminal is located on a foreign network. Triangulation and IP tunneling are difficult to integrate with RSVP.

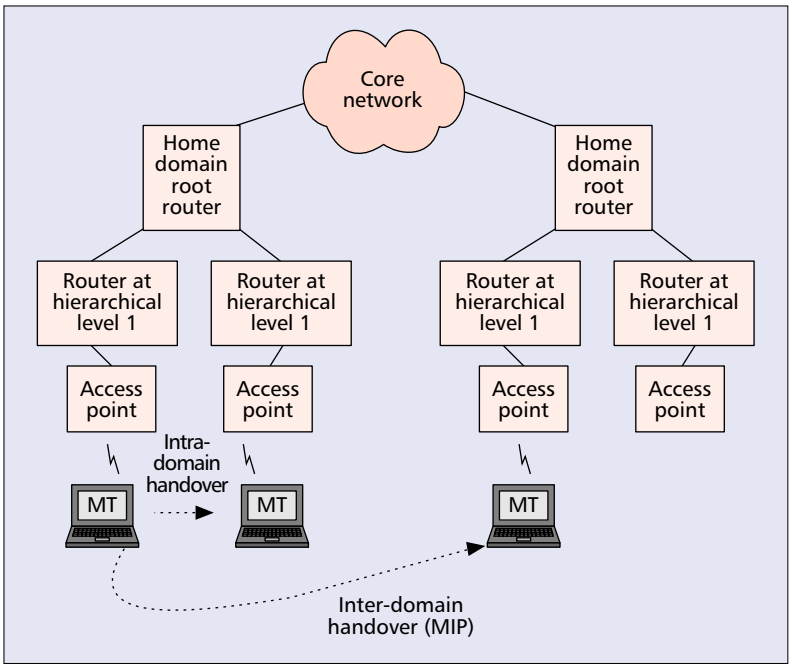

Figure 3. *HAWAII architecture.*

aware of the location of specific terminals. As such, routing outside a domain is performed as in MIP (i.e., per IP subnet); within a domain routing is performed per-terminal using direct routes (i.e.; the terminal keeps its HAddr as before without any triangulation or IP tunneling). The HAWAII network architecture is depicted in Fig. 3.

In HAWAII each domain is structured according to a hierarchy of nodes, forming a logical tree. Each domain owns a root gateway called the domain root router, which takes the role of HA. Each terminal has an IP address and a home domain. Whenever the terminal moves within its domain, its IP address is retained. Packets destined to the mobile terminal are routed to the home domain root router in the normal way based on the IP subnet address of the domain. The received packets are then forwarded to the terminal by using special dynamically established paths. The establishment of these paths is triggered by the mobile terminal by means of the usual MIP registration messages whenever it moves between two APs, as each AP behaves as a different FA. Within the home domain, these messages create direct routing entries in the intermediate nodes they cross.

When the terminal moves to a foreign domain, the usual MIP procedure is used where the foreign domain root router is now the FA, responsible for assigning a CoAddr and forwarding the packets to/from the mobile terminal.

CELLULAR IP

In both MIP and HAWAII layer-3 handover procedures are triggered by MIP signaling such as RFC 1256 when the terminal is already using the new access point. In this way the latency of layer-3 handover may be high, originating significant packet losses. Cellular IP (CIP) [4] makes use of layer-2 information regarding access point signal strength in order to predict handover, allowing the terminal to trigger layer-3 procedures earlier. Unlike HAWAII, in which the terminals run MIP, in CIP they must implement specific CIP procedures. The architecture of CIP is depicted in Fig. 4.

Each CIP domain is composed of a number of CIP nodes structured in a tree topology, having a MIP gateway as the root node. CIP nodes can route IP packets inside the CIP network and communicate with mobile terminals through the wireless interface.

The CIP nodes maintain routing and paging caches. The routing caches are used to locate roaming mobile terminals, being updated by the IP packets transmitted by the mobile terminal. Throughout the CIP nodes, a chain of temporary cached records is created to provide information on downlink path of packets destined to the terminal. After a successful roaming procedure, a CIP node can temporarily have several mappings for the same mobile terminal, leading to different interfaces. Whenever a packet arrives at the CIP node destined to the mobile terminal, that packet is sent to all interfaces mapped on the routing cache. Cached mappings must be refreshed periodically by the terminal, otherwise they expire and are deleted.

The paging caches are maintained by paging-update packets sent to the nearest access point each time the mobile terminal moves. These records are created by mobile terminals that do not send or receive packets frequently.

Within the CIP domain, when the terminal approaches a new access point, it redirects its outgoing packets from the old access point to the new access point, updating the routing caches all the way up to the gateway. All packets destined to the mobile terminal are forwarded to both access points during a time interval equal to the routing cache timeout. After the old path expires, the packets destined to the mobile terminal are only forwarded to the new path. As such, when the terminal has no packets to send during handover, it has to generate route-update messages in order to allow correct updating of the routing caches. Between CIP domains, normal MIP procedures are used for macromobility.

It should be noted that in CIP all packets generated within the CIP domain must be routed by the gateway, even if the destination is located in a position adjacent to the source.

TERMINAL INDEPENDENT MOBILITY FOR IP (TIMIP)

All IETF proposals for IP mobility require the mobile terminals to use a mobility-aware protocol stack, as it is the mobile terminal that notifies the access network about handoff by means of special IP layer signaling. This prevents terminals with legacy IP protocol stacks from taking advantage of mobility even when they are attached to a mobile access network. To replace the protocol stacks of all legacy terminals can be a hard task if we consider the variety of mobile terminal operating systems and versions. Coupling the IP layer with layer-2 handoff mechanisms at the APs by means of a suitable interface

avoids the need for special IP layer signaling between the terminal and the AP. Such is the approach followed by Terminal Independent Mobility for IP (TIMIP).

In order for a terminal to be recognized by the TIMIP network, it has to be registered. This is accomplished offline through management procedures. The ANG keeps information on all mobile terminals recognized by the mobile network. For each terminal, this information consists on the following:

- MAC address
- IP address
- MIP capability
- IP address of the MIP home agent
- Authentication key
- Authentication option

The MIP capability parameter specifies if MIP is required, either implemented at the ANG on behalf of the legacy terminal (surrogate MIP) or implemented at the terminal itself. If the terminal has a legacy IP protocol stack, the next two parameters specify respectively the IP address of its home agent and the authentication key to be used between the terminal and the ANG when the authentication option is turned on. It should be noted that TIMIP authentication is mandatory for macromobility scenarios for both MIP and legacy terminals. The IP address of the home agent is not used when the terminal implements MIP, as the terminal itself is responsible for registering with the home agent, bypassing the ANG.

Once this data is configured at the ANG, it is forwarded to the APs (except the authentication key) so that they are able to know the IP address of newly associated terminals based on their MAC address provided by layer-2, as explained below.

POWER-UP

When a MT first appears in a TIMIP domain, a routing path is created along the hierarchy of ARs, as shown in Fig. 5.

The creation of the routing path takes the following steps:

1. The MT performs a layer-2 association with an AP that belongs to the local TIMIP domain.
2. At the AP, layer-2 notifies the IP layer about the presence of the MT in its wireless interface, triggering the routing reconfiguration procedure. Layer-2 sends the MAC address of the terminal to the IP layer. The MAC address is matched against the terminal registration information broadcast by the ANG and the respective IP address is found. As the new AP currently has no routing table entry for the MT, the routing table is updated with the addition of this new entry.
3. The new AP sends a **RoutingUpdate** message up to the AR at hierarchical level 2. This AR acknowledges with a **RoutingUpdateAck** message, and updates its routing table accordingly with the addition of a new entry relative to the MT. This entry points to the source of the **RoutingUpdate** mes-

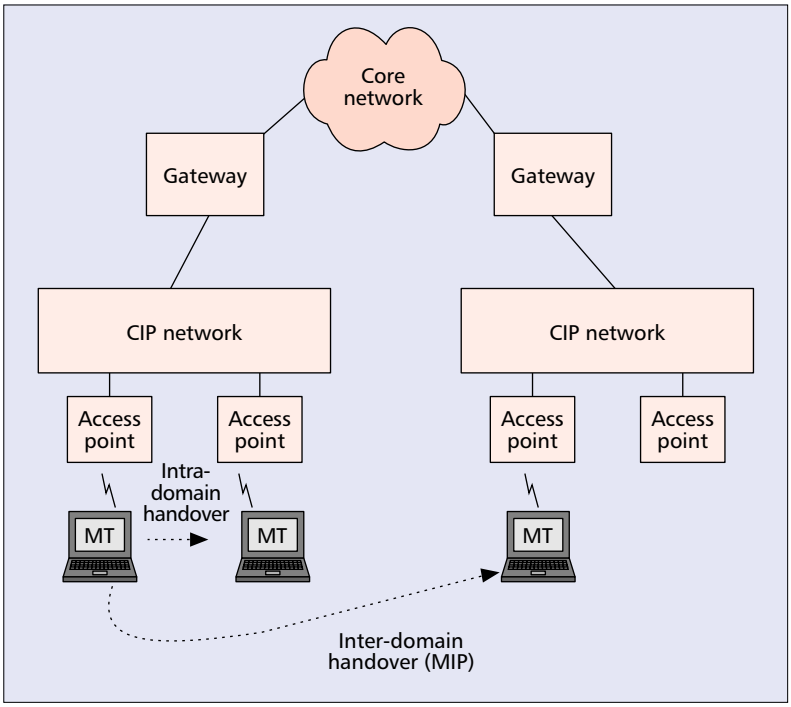

Figure 4. *CIP architecture.*

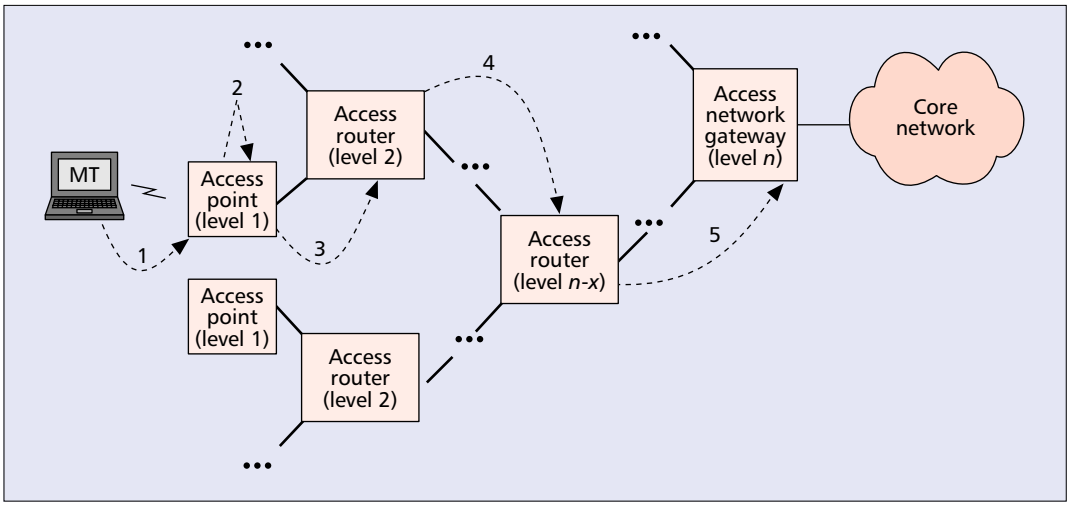

Figure 5. *Establishment of routing path after power-up in a TIMIP domain.*

This basic TIMIP configuration is adequate to have micromobility in wireless access networks where security is not an issue. Nevertheless, just like in other unprotected IP networks, it allows MTs to power-on with false MAC and IP addresses.

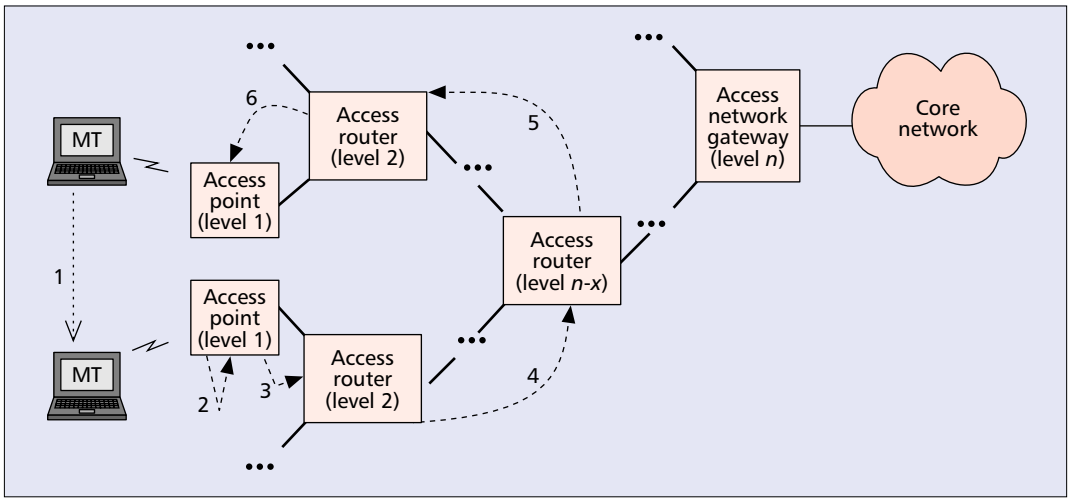

Figure 6. *Routing reconfiguration during handoff.*

sage (in this case the AP) in order to specify the path through which the terminal can be reached.

4. Exchange of **RoutingUpdate**/**RoutingUpdateAck** messages climbs up the hierarchy levels. At each level the routing table is updated with the creation of a new entry relative to the MT. This entry always points to the source of the **RoutingUpdate** message in order to specify the path through which the MT can be reached.
5. Exchange of **RoutingUpdate**/**RoutingUpdateAck** messages reaches the ANG, completing the creation of the new routing path.

The MT is now reachable through the routing path established by the above procedures. The ARs that do not belong to this path have no routing entry for the MT. At these ARs all packets destined to the MT are forwarded up the hierarchy of routers by default. All packets that arrive at an AR whose routing table has an entry to the destination are forwarded down the hierarchy of routers until they reach the radio interface in which the MT is located. Packets destined for a terminal located in the same TIMIP domain as the source reach the ANG only in the worst case.

The **RoutingUpdate** and **RoutingUpdateAck** messages include a timestamp generated at the new AP. As in TIMIP all APs are synchronized by means of the Network Time Protocol (NTP) [5]; this guarantees consistency even when the MT moves faster than the route reconfiguration.

It should also be noted that the routing path is soft-state, and after its establishment it is refreshed by the data packets sent by the MT. Nevertheless, as the packets are routed within the TIMIP domain, some of the ARs may not be refreshed. When this occurs, the routing entry for the MT becomes invalid after a predefined timeout (e.g., 10s). The AR where the timer expired starts to send ICMP **EchoRequest** messages to the terminal, filling the source address field of the IP header with the IP address of the ANG. This forces the MT to reply with **EchoReply** messages destined to the ANG, which will refresh the routing path within the TIMIP domain. If the MT does not reply within a predefined timeout (e.g., 60s), the routing entry for the MT is removed.

This basic TIMIP configuration is adequate to have micromobility in wireless access networks where security is not an issue. Nevertheless, as in other unprotected IP networks, it allows MTs to power-on with false MAC and IP addresses. In order to avoid this, a minimal security functionality must be implemented at the MT itself. However, this can be done in the application layer with no need to change the IP protocol stack. When the authentication option is turned on, it is assumed that the MT runs a special security application, which uses a database of authentication keys for the different TIMIP domains in which the MT is allowed to power-up. This database is indexed by the IP addresses of the ANGs that are the root of the respective networks. The authentication takes place in step 2 of the power-on procedure, immediately after layer-2 notifies the IP layer of the AP about the association of the MT. The AP sends a **SignatureRequest** message to a well known UDP port in the MT. This message carries <IP address of the MT, IP address of the ANG, *rand*, timestamp>, where *rand* is a random value and the timestamp is an NTP-formatted 64-bit value. The same message is sent to the ANG. Both the MT and the ANG answer the AP with a **SignatureReply** message containing the same fields present in the **SignatureRequest** message, plus its 128-bit MD5 message digest [6] calculated with the authentication key of the MT for this network. The latter is only known by the MT (based on the authentication key database and the IP address of the ANG) and the ANG (based on the registration information). The AP compares the signatures of the two **SignatureReply** messages, and proceeds with the routing reconfiguration procedures in case there is a match.

Micromobility

Handoff between two APs that belong to the same TIMIP domain is depicted in Fig. 6.

The first four steps of the handoff procedure are the same as those of the power-up proce-

dure. The remaining steps are as follows:

5. Exchange of **RoutingUpdate**/**RoutingUpdateAck** messages climbs up the hierarchy levels, until the crossover AR (the AR that belongs simultaneously to the old path and to the new path) is reached. Now that the new routing path is completely created, the old path must be deleted. This procedure starts when the crossover AR sends a **RoutingUpdate** message addressed to the MT through the old routing path. The AR that receives the message realizes that the MT is no longer accessible through it, updates its routing path by deleting the entry that corresponds to the MT and replies with a **RoutingUpdateAck** message.
6. Exchange of **RoutingUpdate**/**RoutingUpdateAck** messages goes down the AR tree following the old path, until the Old AP is reached. At each level, the routing table is updated by deleting the entry relative to the MT.

A problem might arise due to the fact that a TIMIP domain consists of a single IP subnet. In a normal shared media LAN, when a terminal has a packet destined to an address within the same IP subnet (which is known through the analysis of the IP address prefix), it tries to obtain the MAC address of the destination through an ARP request before sending the packet directly to it. In TIMIP, as the APs have the functionality of routers, if the destination is associated with a different AP (and hence a separate wireless interface, though in the same IP subnet), the ARP request will not reach its destination. In order to prevent this situation, the MT must be forced to address all MAC frames to the local AP, which in turn will route them properly to their destination. A simple implementation is to have the APs answer to the ARP requests on behalf of the target MTs with their own MAC address. Nevertheless, this is a complex task and can lead to an increase of the traffic broadcast within the radio interfaces due to the ARP messages. It is preferable to configure the MTs with a special subnet mask of 255.255.255.255 and the ANG as the default router to force the MT to send all IP data to the ANG, and to have the APs performing proxy ARP of the ANG with their own MAC address.

MACROMOBILITY

Similarly to HAWAII and CIP, TIMIP relies on MIP to support macromobility. The ANG implements the home agent (HA) for MTs whose home network is its TIMIP domain. The ANG implements surrogate MIP on behalf of foreign legacy terminals and the role of the foreign agent (FA) for foreign terminals that support MIP.

Macromobility for Legacy Terminals — When a MT enters a TIMIP domain different from its current location, the terminal is locally authenticated and a routing path is created between the terminal and the ANG. Packets are then sent/received to/from the outside through the ANG. If the home network of the MT is a different MIP domain, its HA must be notified so that packets can be correctly routed through an IP tunnel established from the HA to the FA located at the ANG.

After consulting the registration information of the MT (namely the IP address of the HA and the MIP capability), the ANG realizes that it is a foreign MT and that it does not implement MIP. Consequently, the ANG must act as a MIP proxy on behalf of the MT, generating all MIP signaling as the MT would. First it must notify the HA about the MT's new location and CoAddr by means of a MIP **Registration Request** message, which requires authentication using the authentication key between the MT and the HA. As the ANG does not know this key, it is the MT that must sign the message. The ANG sends the MT an **AuthenticationRequest** message containing <IP address of the ANG, IP address of the HA, MIP **Registration Request**, timestamp> authenticated by the ANG with MD5(*K1*, **AuthenticationRequest**), where *K1* is the authentication key between the MT and ANG for this TIMIP domain. The MT finds *K1* in the key database based on the IP address of the ANG and obtains the authentication key of its home network (*K2*) in the key database, based on the IP address of the HA. It then answers with an **AuthenticationReply** message containing <IP address of the ANG, IP address of the HA, MD5(*K2*, MIP **Registration Request**), timestamp>. This message is also authenticated by the terminal with MD5(*K1*, **AuthenticationReply**). The ANG can now send a correctly authenticated MIP **Registration Request** message to the HA adding the message digest provided by the MT as a mobile-home authentication extension field. The HA answers with an authenticated MIP **Registration Reply** message, which has a message digest MD5(*K2*, MIP **Registration Reply**) appended as a mobile-home authentication extension field. In order to verify the identity of the HA, the ANG must again rely on the MT. It sends an **AuthenticationRequest** message to the MT, containing <IP address of the ANG, IP address of the HA, MIP **Registration Reply** (except the mobile-home authentication extension), timestamp>, authenticated with MD5(*K1*, **Authentication Request**). The terminal answers with an **AuthenticationReply** message containing <IP address of the ANG, IP address of the HA, MD5(*K2*, MIP **Registration Reply**), timestamp>. If the MD5 digest of the MIP **Registration Reply** provided by the MT matches that present in the mobile-home authentication extension of the **Registration Reply** message sent by the HA, the ANG can resume communication with the HA.

After the communication with the HA is established, the ANG de-encapsulates the tunneled IP packets that come from the HA addressed to the MT and forwards them normally to the MT according to the routing path established in the AR tree. Packets generated by the MT are routed normally according to the same procedures described above for micromobility.

As was already seen, all traffic that crosses the boundary of the TIMIP domain must pass through the ANG, which is the IP gateway to the

When a MT enters a TIMIP domain different from its current location, the terminal is locally authenticated and a routing path is created between the terminal and the ANG. Packets are then sent/received to/from the outside through the ANG.

After a routing path is updated due to handoff, context information pertaining to the active IP flows must be transferred in order to assure seamless mobility. This context information can be related to security, header compression, QoS, and so on.

core network. Nevertheless, whenever an MT moves to a different domain, the IP address of the ANG changes. In order to keep consistency, the MT must change its IP gateway configuration at each handoff between TIMIP domains, otherwise the ARP requests to obtain the MAC address of the IP gateway would not be answered by the APs. This inconvenience is avoided by configuring the MTs with a well known ANG IP address recognized by all APs of all TIMIP domains. The latter broadcast gratuitous ARP messages associating their own MAC addresses with the well known ANG IP address each time a terminal performs an association.

Macromobility for MIP Terminals — When the MT supports MIP but belongs to a different domain, the ANG plays the role of FA. The MT powers-on in the same way as legacy MTs, which makes it mandatory for it to have the TIMIP authentication application installed. Once this is completed, the MIP signaling starts. The ANG broadcasts RFC 1256 **Router Advertisement** messages periodically, specifying its IP address as the MIP CoAddr. In order to hasten the process, the MT can request the advertisement by broadcasting a **Router Solicitation** message, which is then forwarded by the AP to the ANG.

After the MT receives a **Router Advertisement** message, it notifies its HA about the CoAddr through the ANG. The HA is then able to forward the incoming packets to the CoAddr through an IP tunnel. The ANG de-encapsulates the IP packets and forwards them normally to the MT according to the routing path established in the AR tree. Packets generated by the MT are also routed normally within the TIMIP domain. Handoffs between APs within the foreign TIMIP domain are handled with TIMIP micromobility procedures (see above) as the FA is always the same (i.e., the ANG).

It should be noted that in this case it is the MT itself that authenticates the MIP messages when communicating with the HA.

Context Transfer

After a routing path is updated due to handoff, context information pertaining to the active IP flows must be transferred in order to assure seamless mobility. This context information can be related to security, header compression, QoS, and so on. The context transfer solution currently used in TIMIP is compatible with the Context Transfer Framework for Seamless Mobility [7] recently proposed in the SeaMoby working group of IETF. According to this framework, the MT signals handoff to the New AP by means of a **Seamless Handover Initiate (SHIN)** message in which it provides the IP address of the old AP among other relevant information. The new AP answers with a **Seamless Handover Acknowledgement (SHACK)** message. It then requests context information about the MT from the old AP sending an ICMP message with a **Seamless Handover Request (SHREQ)** option. Upon receiving this message, the old AP sends the requested information in a **Seamless Handover Reply (SHREP)** option in an ICMP message directed to the new AP. The old AP can also send this context information without receiving any request by means of an **Unsolicited SHREP (U-SHREP)**. A slight modification is required to support legacy terminals. As the latter have no support for mobility signaling, they cannot provide the address of the old AP to the new AP (or vice versa) in a **SHIN/SHAK** exchange, as would be required for the **SHREQ/SHREP** context transfer. In this case, the old AP is configured to send a **U-SHREP** message addressed to the terminal once the new routing path is established. This message eventually reaches the new AP, where it is intercepted. The new AP acknowledges context transfer, sending a **SHREP-Ack** message to the old AP whose IP address is obtained from the **U-SHREP** message.

Conclusions

This article has presented a new proposal for mobility in IP networks called Terminal Independent Mobility for IP (TIMIP). In TIMIP, power-on and handover are inferred from layer-2 notification at the wireless access points. Consequently, IP mobility signaling is completely implemented in the network nodes and thus transparent to the IP layer of the terminals. Although authentication still requires some functionality to be performed at the terminals, it can be implemented as an independent application with no impact on the IP protocol stack. This contrasts with the CIP and HAWAII solutions proposed to the IETF that require the IP protocol stack of the mobile terminals to be changed to support special mobility signaling, which can be a hard task if we consider the variety of mobile terminals, operating systems, and versions available.

TIMIP combines some advantages from CIP and HAWAII. Like CIP, refreshing of routing paths is performed by data packets sent by the mobile terminals, with signaling being employed only when no traffic is detected at the routers for a certain time interval. Like HAWAII, routing reconfiguration during handoff within a TIMIP domain only needs to change the routing tables of the access routers located in the shortest path between the new AP and the old AP. Another feature similar to HAWAII is that routing of data packets within a TIMIP domain does not need to reach the access network gateway, involving only the access routers located in the shortest path between the sender and the receiver.

Preliminary tests in a simple configuration with two APs and one ANG have shown that handoff latency due to TIMIP is not higher than 4 ms, which is satisfactory given the fact that the APs and the ANG used in the tests were based on PCs running LINUX with a TIMIP user-space implementation. Test scenarios with more network nodes will be performed in the near future.

Acknowledgments

The work presented in this article has been performed in the framework of IST project IST-2000-25137 MOICANE (<http://www.moicane.com>), which is partly funded by the European Union. The authors alone are responsible for the content of the article.

References

[1] IETF, "IP Mobility Support," RFC 2002, Oct. 1996.
[2] IETF, "ICMP Router Discovery Messages," RFC 1256, Sept. 1991.
[3] R. Ramjee *et al.*, "IP-Based Access Network Infrastructure for Next-Generation Wireless Data Networks," *IEEE Pers. Commun.*, vol. 7, no. 4, Aug. 2000.
[4] A. Campbell *et al.*, "Design, Implementation and Evaluation of Cellular IP," *IEEE Pers. Commun.*, vol. 7, no. 4, Aug. 2000.
[5] IETF, "Network Time Protocol (Version 3), Specification, Implementation and Analysis," RFC 1305, Mar. 1992.
[6] IETF, "The MD5 Message-Digest Algorithm," RFC 1321, Apr. 1992.
[7] IETF, "A Context Transfer Framework for Seamless Mobility," Internet draft, draft-koodli-seamoby-ctv6-01.txt, July 2001.

Biographies

ANTONIO M. GRILO (amg@cris.inesc.pt) received the information technology engineer degree in 1996 and the M. Sc. degree in electronics engineering and computers in 1998, both from the IST, Technical University of Lisbon, Portugal. He is currently doing his Ph. D. course work at the same institution, working in the area of wireless access networks. He is an assistant professor at IST, where he has been teaching digital systems and telecommunications since 1998, in graduate and post-graduate courses. In 1995 he joined INESC, Lisbon, working in the area of broadband access networks and terminal equipment. Since 1996 he has been working in several european projects, namely the ACTS projects ATHOC and AROMA, and is currently participating in the IST project MOICANE.

PEDRO V. ESTRELA received the information technology engineer degree in 2000 from the IST, Technical University of Lisbon, Portugal. He is currently doing his M. Sc. course work at the same institution, working in the area of IP mobility and QoS support for wireless hosts. In 1999 he joined INESC, Lisbon, working in the area of terminal equipment and access networks. He has currently participating in the IST project MOICANE.

MARIO S. NUNES received the electronics engineer degree in 1975 and the Ph. D. degree in electronics engineer and computers in 1987, both from the IST, Technical University of Lisbon, Portugal. Since 1975 he has been an associate professor at IST, where he teaches digital systems and telecommunications in graduate and postgraduate courses. In 1980 he joined INESC, Lisbon, where he is now a group leader, working in the area of broadband access networks and terminal equipment. Since 1988 he has been responsible for the INESC participation in several european projects, namely the RACE projects "Technology for ATD" and EXPLOIT, and the ACTS projects ATHOC and AROMA. He is currently participating in the IST project MOICANE. He is the author of two books: *Digital Systems* and *Integrated Services Digital Networks*.

Preliminary tests in a simple configuration with two APs and one ANG have shown that handoff latency due to TIMIP is not higher than 4 ms.