WiFi mobility framework supporting GPRS roaming: Design and Implementation

A.Calvagna, G.Morabito, A.Pappalardo

Dipartimento di Ingegneria Informatica e delle Telecomunicazioni
University of Catania
V.le A. Doria 6, 95125 - Catania (ITALY)
Email: andrea.calvagna@unict.it

***Abstract*— To provide IP mobility for wireless users several *micro-mobility* protocols are currently available. These are capable of supporting this feature inside the scope of a LAN, by means of performing *handovers* between adjacent WiFi radio-access cells in order to follow users' movements. Also, it is possible to achieve wireless mobility in a larger extent, i.e. across whole network domains. But, in order to do it these protocols have to be used in conjunction with a *macro-mobility* protocol, like Mobile IP. In this context, a problem arises if such domains are so far away from each other that wireless-access *gaps* exist between them. In fact, this prevents wireless IP users from experiencing access continuity while traveling across these domains. In this paper we describe a solution which was designed and implemented to cope with the above problem. Starting from the Cellular IP protocol, we developed a new mobility framework that extends it to seamlessly manage roaming into GPRS access network, whenever the mobile host is out of range from any WiFi domain. Also, management of inter-domain macro-mobility is integrated in our framework, eliminating the need to externally rely on Mobile IP.**

I. Introduction

As advances in microelectronic allow for palm-sized computers and low-cost wireless interfaces, users' interest in experiencing true wireless mobility with IP devices is growing faster than ever. IP-mobility protocols *must* enable maintenance of established sessions without significant service disruption while not restricting the movements of mobile users to single points of attachment or subnetworks [4]. Thus, much research work is currently undergoing to support wireless/mobile IP access and inter-working with the fixed-Internet (see [8], [1], [11]). As a result, nowadays several approaches to mobility management are available, usually referred to as *micro-* and *macro-mobility*: in a **Macro-Mobility** context the *Mobile Host* (MH) can access. the Internet from any foreign subnet offering an available access point while preserving its identity. Mobile IP [9] supports this type of mobility. However, it does not support seamless or near-seamless mobility due to the inefficient location updating during handovers. Complementarily, a **Micro-Mobility** framework supports seamless or near-seamless wireless mobility for users within the same subnetwork. The considered wireless access network is organized in cells, each covered by a WiFi (IEEE 802.11b) access point. The MH can communicate while moving across radio cells spatially adjacent with each other. *Cellular IP* (CIP) [2] and other solutions (see [5], [10]) has been proposed to support such mobility. Let's define *Cellular WiFi domain* (simply *WiFi* domain, hereafter) the area covered by a set of contiguous WiFi cells belonging to the same IP subnet. According to this definition, current micro-mobility protocols handle mobility within a WiFi domain, and then rely on Mobile IP to handle cross-domains mobility, assuming adjacent domains. But, in real life, it may be common to face network scenarios where several disjunct WiFi domains coexist within the same network. An example of this scenario comes from our University Campus which consists of several sites, which are also WiFi domains, spread across the whole city area. Despite the fact that they are already networked together to form a single wired-cum-wireless MAN, their reciprocal distance is too high to allow wireless access continuity for users moving from one site to another (e.g., professors teaching Computer Science in different departments). As a consequence, wireless users exiting a site experience forced tear down of all active TCP connections. At present, General Packet Radio Service (GPRS) access is available almost everywhere, thus it can be used to fill the wireless access *gap* between disjunct WiFi domains. Indeed, in the considered scenario macro-mobility features must also be involved to enable roaming of MHs into the foreign WiFi domains they traverse. In this paper we describe the middleware we designed and implemented to cope with the above problem, that is, to provide uninterrupted wireless IP connectivity to users moving between distant WiFi domains, seamlessly switching between Cellular IP-like WiFi mobility and GPRS roaming. This allows mobile users to experience the benefits of wireless access to their private data and personal services while on the move across the city campus. Of course, services running over a GPRS link experience a dramatic decrease in bandwidth and increase in latency, but (at least) keep up and running. This can be even more significant if we consider that most of the time users connect to non real-time services, like web or email. The rest of this paper is organized as follows: the proposed solution is described in Section II and assessed in Section III. Our conclusions are drawn in Section IV.

0-7803-7802-4/03/$17.00 © 2003 IEEE

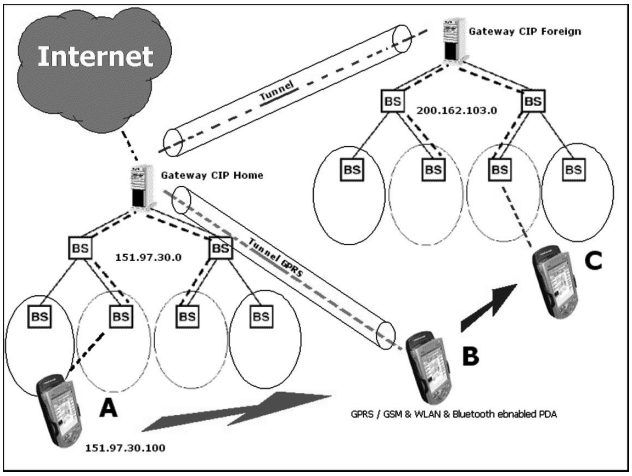

Fig. 1. Considered system scenario: MH moves out from its home domain (A) toward a distant foreign domain (C), preserving connections to the Internet through GPRS meanwhile(B).

II. System Description

In this section we describe the middleware we designed and implemented to allow access continuity in the scenario depicted in Figure 1. The middleware, called *WiFi Bridge*, is based on improvements of open-source CIP, that is, enhancements of the protocol stacks implemented at the GW and MH to support newly introduced roaming features. More in detail, we describe the major characteristics and the novelties introduced in the gateway (GW) and MH in Sections II-A and II-B. Moreover, the roaming procedures inside GPRS and foreign WiFi domains and the system behavior in case of *inter-domain* handover, that is, WiFi to GPRS and viceversa, which are the new features enabled by *WiFi-Bridge*, will be presented in Section II-C, II-D and II-E, respectively.

A. The Mobile Host

We used as MH a PDA device (Ipaq 3870) running Linux kernel v2.4. Thanks to an 802.11b (WiFi) PCMCIA NIC installed on it, the MH is able to gain IP connectivity while moving around into any WiFi domain. MH is also capable of integrated *Bluetooth (BT)* connectivity, over which it creates a PPP connection to a *BT* enabled GPRS/GSM mobile phone, to gain GPRS access. Thus, MH advantages the availability of two radio interfaces, WiFi and GPRS, seamlessly switching between them when appropriate in order to avoid loss of IP connectivity. In fact, when the user brings its MH outside the radio boundaries of its home WiFi domain the device will automatically detect a loss of WiFi signal and, as a consequence, will divert all IP connections to the GPRS access interface. In general, the connections are carried through the GPRS access network when WiFi access is not available, but are seamlessly carried back to the WiFi interface as soon as WiFi access point signal is available. A newly introduced WiFi Mobility Management (MM) thread has been implemented on the MH specifically to manage the task of relating IP to the most appropriate access solution which is chosen analyzing the information gathered by the protocol.

B. Gateway Functionalities

In *WiFi Bridge* the Gateway node, in addition to micro-mobility management tasks derived from the CIP GW, is responsible for the following new functionalities:

- *Registration Management*. Let G_i be the Gateway of the i-th WiFi domain, $WiFi_i$, and let Ψ_i be the set of MHs whose home domain is $WiFi_i$. A visiting MH x, $x \in \Psi_j$ with $i \neq j$, must initiate a Registration procedure in order to obtain access in $WiFi_i$. This is done by sending an appropriate request to G_i, which will ask some information to the Gateway of the home network of x, G_j. Therefore, the generic Gateway G_i takes part in two types of Registration procedures:
  1) The Registrations of the visiting MHs that want to obtain wireless access in $WiFi_i$.
  2) The Registrations of the MHs belonging to Ψ_i that want to obtain wireless access in foreign WiFi domains.
- *IP Tunnel Management*. *WiFi Bridge is based on IP tunneling*. At least one of the end-point of any IP tunnel is always a Gateway.
- *Packet Classification*. The Gateway G_i must distinguish the packets:
  - coming from an IP tunnel, destined to a certain MH.
  - destined to a MH belonging to Ψ_i, which is currently visiting a foreign $WiFi$ or is only reachable through GPRS.
  - generated by MHs visiting $WiFi_i$.
- *Packet Forwarding*. The Gateway G_i must forward the packets destined to MHs belonging to Ψ_i which are currently outside $WiFi_i$ and the packets generated by MHs visiting $WiFi_i$ towards the appropriate IP tunnel.

C. Roaming into GPRS domain

WiFi Bridge is based on the establishment of appropriate IP tunnels from our *enhanced* version of CIP Gateway (GW) and the MHs. The MH receives a dynamic IP address valid in the GPRS domain. This is done within the registration procedure executed when the MH is turned on. This dynamic IP address is provided to the Home GW which maintains updated an appropriate cache, called *tunneling cache*, containing information about the mapping between the static and dynamic IP addresses of the MH. Then, an IP tunnel is established between the Home GW and the MH (identified by means of its dynamic IP address). Lets call this the *GPRS-Tunnel*. Observe that, although this tunnel is always present, it remains inactive as long as the MH is within a WiFi domain. A MH is outside any WiFi domain when there are not WiFi base stations in the proximity. This can be easily recognized because, according to Cellular IP, WiFi base stations transmit a *beacon signal*. Therefore, the fact that the MH cannot listen any beacon signal (or the level of the signal is too low) is the evidence that the MH is outside any WiFi.

D. Roaming into foreign WiFi domain

When the MH is visiting a foreign WiFi, another IP tunnel is established between the home and foreign gateways of the two involved networks. Down-link IP traffic destined to the MH, thus arriving to its home GW, will be forwarded through this specific tunnel interface directed to the right foreign GW. This latter will in turn route down-link traffic to the MH's current position inside its domain, based on standard micro-mobility paging cache info. Lets call this tunnel *Bridging-Tunnel*. Note that only one of these tunnel bindings is needed between any WiFi(GW) pair, since it's then shared between all the MHs belonging to the one but migrated to the other, regardless of how many MH they are. Also these tunnels expire (their entries are removed from GW's tunnel caches) if no migrated MH exist anymore in the corresponding WiFi domain. On the contrary, a *bridging-tunnel* set-up is triggered by the first MH (re-)entering in the considered foreign WiFi. Obviously, before such a tunnel is set-up the registration of the MH in the foreign WiFi occurs, involving an authentication procedure which is based on MH's MAC address validation (by querying the home GW).

E. GPRS/WiFi handoff behavior

In this paragraph we explain the system behavior when a MH performs a handoff from its home WiFi domain to GPRS, and back on. There are four main *connection phases* the MH experiences, which we are going to highlight in the following:

1) WiFi: In this phase the MH is located inside its own home WiFi domain, and its mobile connectivity is managed by the domain's GW normally, as in CIP. MH sends and receives packets through the WiFi interface and, moreover, periodically sends *paging-update* messages toward the local GW to let it constantly track its current location inside the domain.

2) WiFi to GPRS: Here the mobile host steps outside of its home WiFi domain radio range. No other WiFi domain is present to offer connectivity, so it sets as default route for outgoing packets the GPRS tunnel interface to its Home GW, actually performing a *hard handoff* from WiFi to GPRS access network. The MH sends as first message on the GPRS tunnel a *gprs-solicit* message, followed by its up-link IP data traffic. In response to the solicit message, the Home GW sets also its endpoint of the GPRS tunnel as default forwarding interface for MH's down-link packets.

3) GPRS: In this phase the IP tunnel interface, linking the MH and its home GW through GPRS network, is used by the MH as forwarding interface, so packets may flow normally to their destination. During this phase the state of the WiFi Mobility Management (MM) thread on the MH is freezed, including its internal *paging-update* timer, to be waken later when stepping back inside the WiFi domain;

4) GPRS to WiFi: This phase of the cycle represents the MH stepping back inside its home WiFi domain. Start of this phase is triggered in the MH by the reception of the first *beacon* advertisement message, coming from the nearest in-range BS of the WiFi domain. This message provokes the *awakening* of the MM thread inside MH, that resumes its execution and consequently sets that advertising BS' IP address as default route for its uplink packets. After this, the MH still keeps on receiving UDP packets from the GPRS tunnel. In fact, it still has to wait for the expiration of last resumed *paging-update* timer before it can expressly signal its presence to the WiFi Home Gateway, sending a *paging-update* message. As soon as the home GW receives the *paging-update* message it sets-up default route toward the MH back to the WiFi domain route. Due to the fact that a *soft handover* is actually performed, the MH receives IP packets from both access interfaces, WiFi and GPRS, for the brief period of time intervening between the awakening of the MM thread in the MH and the actual update in the GW of the routing path to MH.

III. System Evaluation

To evaluate our middleware we built a testbed and designed a set of experiments, by means of which. The goal of the experiments is to analyze the performance of the protocol. In what follows we describe the testbed and tests results. The most interesting case study is certainly the handoff between WiFi domain and the GPRS network, since it may experience packet losses and it represents a case not contemplated in the original version of the Cellular IP. Performance tests on roaming functionality for MH coming into foreign WiFi domains have not been taken into account since in that case, after authentication phase, our framework performs a standard handover procedure, which has already been evaluated in [3].

A. Test environment

The experimental results reported in this paper are based on measurements taken from the testing environment we realized. The test network topology consisted in two different subnetworks, implementing WiFi domains, which will play the role of *Home* domain and *Foreign* domain, respectively, networked by a router. The router also interconnects these domains to a third, fixed subnet, which in turn is connected to the rest of the Internet. Each of the two WiFi domains consist of one CIP Base Station (BS) node and one *enhanced* Gateway (GW) node. All nodes, including the router, are Linux boxes based on multi-homed 350MHz Pentium II PCs hardware. They are all wired using 100Mb/s full duplex Fast-Ethernet links. Mobile Host (MH) is a Compaq iPAQ PDA with Linux 2.4.17, and is also linked with the router by serial cable (PPP over RS232), to emulate GPRS access in the tests. Mobile host and base stations are also equipped with 11Mb/s Orinoco *PCMCIA* WiFi NICs.

B. Testing procedure

The approach taken in the experiments was to investigate the impact of handoffs on UDP performance. Hence, we generated a UDP packet flow between a source host in the fixed subnet and the MH, using the tool *mgen* ([6]), and measured packet losses and packets delays during handoffs from WiFi domain to GPRS, and back on. In fact, during this experiments the MH receives 100 byte sized UDP packets at rates of 25pps,

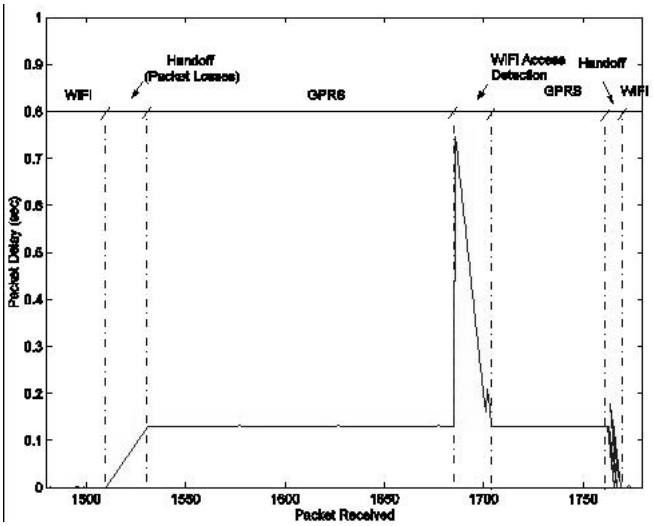

Fig. 2. Packet delay experienced in handoff cycle. Four phases are highlighted: *WiFi access, WiFi to GPRS hard handoff, GPRS access, GPRS to WiFi soft handoff.*

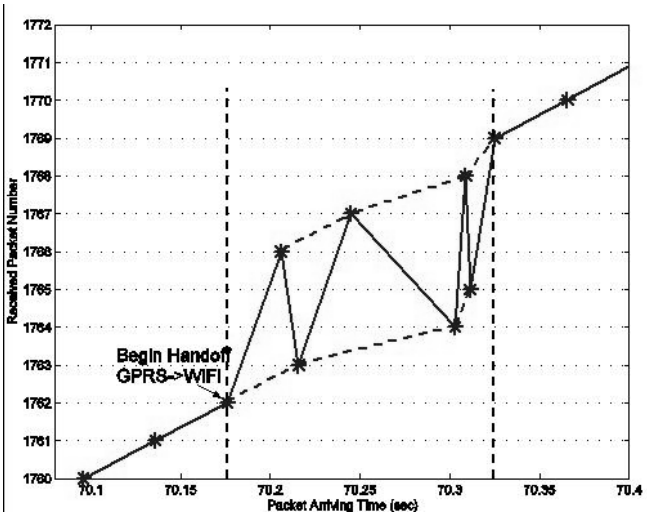

Fig. 3. Packet arrival times during GPRS to WiFi soft handoff showing non sequential packets ordering.

while performing handoff cycles according to this schema: *WiFi to GPRS, 7sec pause, GPRS to WiFi, 7sec pause.* Pauses have been inserted to ensure the system is returned in a steady state before starting next handoff procedure.

C. Delay measurements

In this section we focused on the delivery time for UDP packets (Packet Delay), with regard to the WiFi to GPRS and GPRS to WiFi handoffs, getting indeed some interesting results. Figure 2 shows final results from the handoff cycle test, in which we highlighted the four different connection phases the MH experiences. During initial WiFi connection phase the mobile host is located inside its own local WiFi domain, thus it receives UDP packets through the WiFi interface, experiencing packet delays in the order of 2msec. When the mobile host goes outside of its home WiFi domain radio range, it performs a *hard-handoff* to the GPRS access network. Experienced packet losses at the MH in this phase are in the order of tenths of packets. They depend on the time spent to perform the involved routing update operations in the home GW. During the subsequent GPRS access phase, the packet delay along this route has been artificially increased to emulate real performance of GPRS network. In particular, we used the *nistnet* [7] tool to emulate a bottleneck along the packets route (specifically on the router node R) in order to manually set a Round Trip Time delay (RTT) of about 130ms between MH and the Home GW. After that, we have the GPRS to WiFi handoff phase. The behavior of this phase is rather complex since we can distinguish three different parts in it, as can be seen in the Figure 2. The observed peak in the network end-to-end delay reflects a sudden consumption of resources in the MH after the reception of the first *beacon* packet, due to the MM thread resuming its execution. After that, the MH still keeps on receiving UDP packets from the GPRS tunnel, that is, packet delay falls back to the precedent value until expiration of resumed *paging-update* timer. Indeed, it could be desirable to shorten the overall duration of the GPRS to WiFi handover procedure by resetting the page-update timer at this time, instead of waiting for its pending expiration. On the other hand, we believe it's safer to leave this delay untouched in order to avoid unstable behavior. In fact, otherwise when the MH comes at a domain boundary its MM thread algorithm would indefinitely perform quick handoff back and forth between the two access networks. Last transient concluding the GPRS to WiFi handoff procedure is characterized by oscillations in the packets delays, as shown in Fig.3. In fact, since a *soft handover* is performed, the MH receives IP packets from both WiFi and GPRS access interfaces, for a brief period. Therefore, as they expose different RTT delays, packets are received in non sequential order. In particular, observed late packets are those coming from the GPRS tunnel that were already been forwarded by the GW on the GPRS tunnel when it received the *paging-update* message, and are still not yet all delivered because of the greater tunnel's RTT. Note that as a *soft* handoff has been performed no packet losses are experienced by the MH in this handoff.

D. Packet loss measurements

As already seen in the previous section, packet losses are experienced by the MH only during the WiFi to GPRS Handoff procedure. Thus, we deeply studied packet losses for this case in a test champaign in which we used as varying parameter the RTT between the MH and the WiFi Home GW. The measurement results are plotted in Fig.4. Reported measurements has been obtained by averaging over 50 consecutive test cycles. Moreover, if compared to a standard WiFi handoff, handoff towards GPRS has a greater duration because of the time necessary for the MH to realize it stepped outside the radio boundaries of its home WiFi domain. We will call this delay *alert delay, (Ai)*. It has to be greater than the *beacon_interval* (*Bi*), that is the time between two consecutive *beacon* packets,

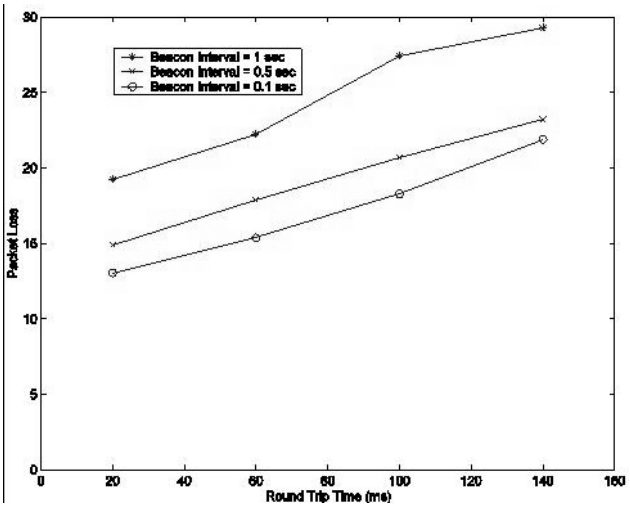

Fig. 4. Packet loss measurements results for the WiFi to GPRS procedure, with respect to varying *Bi* and *RTT* values.

to ensure the MH doesn't misunderstand normal WiFi handoff delay with exit from WiFi domain boundaries. The MH keeps in mind this delay with an internal timer, reset every time that a Beacon Packet is received. This timer expiration is interpreted by the MH as the exit out of the WiFi domain boundaries. Thus, we believed opportune to repeat the measurements also varying another parameter, the *Bi* value. As shown in Figure 4, packet losses are directly proportional to both the values of RTT along the GPRS path and the *Bi* duration, as expected. We have to highlight that, in comparison to the normal *intra-domain* WiFi handoff (see [3]), WiFi to GPRS *inter-domain* handoff causes a greater packet loss (at least in this implementation). This is mainly due to its longer duration, that is, the *alert delay*. However, overall performance could be improved by reducing the *Bi* duration (and as a consequence the alert delay) or with more effective protocol signaling implementations. As an example, in our framework for practical reasons signaling between the GW and the MH has been done through TCP connections, but it probably could have been more effective if based on UDP protocol.

IV. Conclusions

The technical objective reached in the proposed solution is to provide quasi seamless inter-domain handoff between distant CIP domains, by means of a "temporary" GPRS access to the internet. We implemented the proposed framework on linux 2.4.7 environment, starting from Cellular IP version 1.1, and facing a number of interesting problems related to the main objective. In fact, our original contribution consisted in extending the CIP GW and MH functionalities with both *GPRS roaming* support and WiFi *inter-domain* handover management. The proposed middleware has been deployed on a real test-bed and extensively tested. Performance measures show that a service degradation occurs in terms of lost packets when the MH moves from WiFi access domain to GPRS access domain. This is basically due to the bandwidth mismatch between the two environments and the *hard* type of handoff performed, and could be improved by reducing duration of *Bi* timer. Despite of that, access continuity is preserved. As a natural extension to our work we are currently undergoing tests to study scalability implications of the proposed solutions and we also plan to approach the problem of letting applications be aware of currently used network interface in order to adapt, if possible.

References

[1] IST 1999-10054, *Project brain, deliverable d2.2*, `http://www.ist-brain.org`, Mar. 01.
[2] A.T. Campbell A.G. Valko and J. Gomez, *Cellular ip*, Internet Draft, `draft-valko-cellularip-00.txt` (1998).
[3] ———, *On the analysis of cellular ip access networks*, Proc. 6th IFIP International Workshop on Protocols for High Speed Networks , Salem (25-27 August 1999).
[4] J.T. Malinen J. Loughney C. Williams, A. Yegin and A. Mihailovic, *Micromobility problem statement*, Internet Draft, `draft-irtf-mm-prob-stmt-00.txt` (2002).
[5] Claude Castelluccia, *Hmipv6: A hierarchical mobile ipv6 proposal*.
[6] `http://manimac.itd.nrl.navy.mil/MGEN/`.
[7] `http://www.nistnet.org/`.
[8] IST-2000-28584 MIND, *Mobile ip-based network developments*, `www.ist-mind.org`.
[9] C.E. Perkins, *Mobile ip: Design principles and practices*, Addison Wesley, Reading, MA, 1998.
[10] S. Thuel K. Varadhan S.Y.Wang R. Ramjee, T. La Porta, *Hawaii: A domain-based approach for supporting mobility in wide-area wireless networks*, Proc. IEEE International Conference on Network Protocols (1999).
[11] P. Reinbold and O. Bonaventure, *A comparison of ip mobility protocol*, 2001.