Seamless and Uninterrupted Interworking of Wireless and Wireline Network Technologies

Konstantinos Vaxevanakis, Sotirios Maniatis, Nikolaos Nikolaou, and Iakovos Venieris

National Technical University of Athens,
Department of Electrical and Computer Engineering,
9 Heroon Polytechniou str, 15773,
Athens, Greece

{vaxevana, sotos, nikolaou}@telecom.ntua.gr,
ivenieri@cc.ece.ntua.gr

Abstract. The Internet Protocol (IP) dominates in today's data communication infrastructures. The network evolution also favors the explosion of the wireless network technologies. The latter have to be combined and interoperate properly with current wireline installations. Although IP assures interoperability, there are open interworking issues at the session, network, and data link layers related to the nature of the wireless environment. The architecture presented in this paper, proposes specific enhancements to an IP infrastructure, that alleviate the deficiencies of wireless networks and propel the efficient interworking between wireline and wireless network technologies.

1. Introduction

The trend in network evolution is not towards a global and uniform environment. It rather favors the appearance of a combination of wireline and wireless networks that complement each other in terms of coverage area, underlying infrastructure and throughput. In this complicated environment, the Internet Protocol (IP) seems to be the common denominator for the information world. IP services are supported by almost all physical interfaces both in the wireless and wireline worlds, thus realizing interoperability of services.

Designed and operated for many years over wireline infrastructure, IP is not optimized for supporting communications over wireless interfaces. Consequently, IP is not always adequate to offer seamless and uninterrupted operation of a mobile host that moves within the diverse environment that is designated by the mixture of various wireless and wireline technologies.

To start with, the mobile host's IP address reveals location information, thus limiting the operating range of the host within the boundaries of the IP domain this address belongs to. Migration to other IP domains is possible only if the host offers the appropriate mechanisms. Besides, migration to a different IP domain might imply that a modification would occur at the physical layer, too. The seamless and

S. Rao and K.I. Sletta (Eds.): INTERWORKING 2000, LNCS 1938, pp. 326-336, 2000.

uninterrupted roaming between IP domains and physical interfaces is not currently offered by the IP protocol.

Additionally, one major drawback of the wireless networks is that they are susceptible to interruptions of any kind, like short disconnections in case of a temporary signal loss. On the other hand, applications are usually implemented according to the properties of the wireline world, where such phenomena do not exist. Software developers require network transparency, so they cannot be obliged to have the properties of the wireless environment in mind when they design their applications. In order to facilitate end-to-end interconnection and operation – independently of the underlying wireless and wireline infrastructure mixture – specific enhancements to the operation of the IP service must be presented to the wireless side.

This paper introduces an architecture that takes into consideration the aforementioned requirements of the foreseen complicated environment as well as the specific deficiencies of the wireless one, and provides IP-based enhancements in various layers of the OSI model. In this way, applications that exist in wireline environments can be supported in wireless environments too, without any modification, while still efficiently utilizing the basic IP services.

The rest of the paper is organized as follows. Section 2 provides a thorough insight into the proposed architecture. It discusses the functionality of added components, along with the rationale behind them. Section 3 presents a reference environment, which had been setup in order to act as a platform for trials and experiments. Section 4 discusses the results obtained by the trials' execution. Last, Section 5 gives the conclusions and possible future extensions.

2. Proposed Architecture

There are two basic wireless enhancements supported by the architecture, namely the location transparency and the application resiliency to link disconnections. The former refers to the Network and Data Link layers of the OSI model, while the latter belongs to the Session layer. These enhancements are logically placed in the convergence point between the wireless and wireline infrastructures. Physically, the proposed enhancements are introduced in the mobile host as well as in a Gateway/Proxy at the home Intranet.

The address of a node that resides within an IPv4 network, apart from identifying the node itself, contains topological information, thus binding the terminal with a specific location. Consequently, if a mobile terminal attempts to move without changing its IP address, then it will be unable to route packets correctly, while if it dynamically modifies its address, then all active connections will be terminated.

To overcome this problem and allow a mobile terminal to roam freely around the network, while still communicating and maintaining the same IP address, the concept of Mobile IP protocol has been followed. Mobile IP [1] defines two new entities, the mobility agent, which include the Home and Foreign Agent (HA and FA), and the Mobile Host (MH). Mobility agents are located inside the network and are responsible for specific sub-networks, while MH is located inside the mobile terminals. Whenever

the mobile terminal is connected to a foreign sub-network, the Mobility Agent (HA) controlling the home sub-network, forwards all the packets destined for the mobile host to a specific FA that resides within the foreign sub-network. The FA in turn delivers the packets to the mobile terminal. In this manner, although the mobile terminal moves to a different network domain, active TCP/UDP sessions are maintained alive and data packets continue to reach the mobile terminal.

Taking into consideration that location transparency must be provided to the terminal, independent from the underlying wireline or wireless medium, we have concluded to the overall architecture, depicted by Fig. 1. It covers both the terminal and the network side, having part of the functionality of MH and FA supported within the mobile terminal, while its counterpart HA functionality is implemented within the Gateway/Proxy. The mobile terminal is equipped with more than one Network Interface Cards (NICs). At least one of them is wireless, while the others could be either wireless or wireline. Depending on the network environment – indoors (e.g. home, corporate premises/office) or outdoors (e.g. when away from home/office) communications – one of the interfaces is active, while when it is necessary, a switching can be performed from one to the other.

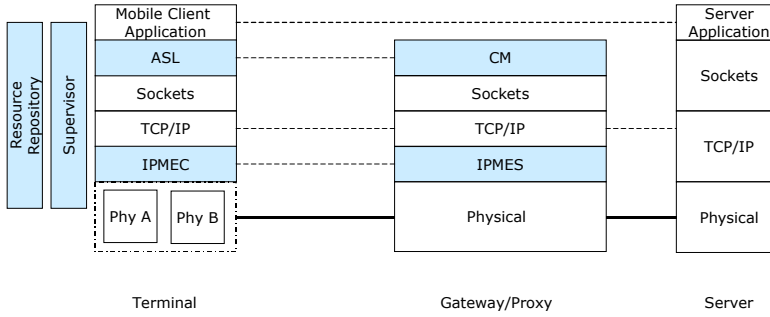

Fig. 1. Proposed Architecture

The IP Mobility Enhancement Client and Server (IPMEC/IPMES) team up with the IP protocol to achieve location transparency and make mobility transparent to higher level protocols (like TCP) and, eventually, to applications.

More specifically, the IPMEC module resides within the mobile terminal and when it is activated it registers with the Gateway/Proxy. IPMEC is mainly responsible for redirecting IP packets over the correct underlying interface. IPMEC has the privilege to modify the routing table of the terminal. More precisely, during switching between physical interfaces, all the routing entries directed over the current interface are deleted and re-directed over the new selected interface.

Whenever the mobile terminal switches from one interface to another, no modification is made with the terminal's IP address. This is one of the prerequisites that enables the terminal to switch between interfaces, without having all the active transport connections terminated. To fulfill this requirement, the IP address of the terminal is either associated with the MAC address of the current interface, or with the MAC address of the Gateway/Proxy. The latter serves the purpose of having the

packets, which are destined to the mobile terminal, received by the Gateway/Proxy, and, subsequently, forwarded to the terminal.

In order to achieve such a behavior, the Gateway/Proxy sends to the network, on behalf of the mobile terminal, ARP (Address Resolution Protocol [2]) packets and updates, accordingly, its routing table. This mechanism of sending ARP packets (Request or Reply [2]) to spontaneously cause other nodes to update their ARP cache, is also known as Gratuitous ARP (GARP [3]).

On the network side, the IPMES component resides in the Gateway/Proxy and implements the complementary functionality of IPMEC. More specifically, following the idea of the Mobile IP mobility agent, it is responsible for the processing of the registration/de-registration messages received from IPMEC. In addition, IPMES caters for the appropriate interception of IP packets from the network and the forwarding of these packets to the proper mobile terminal. Finally, IPMES implements the aforementioned GARP mechanism.

The Abstract Socket Layer (ASL) and Communication Manager (CM) pair of modules provides for the control of the link disconnection for data services. Fig. 2 depicts the operation of these two modules.

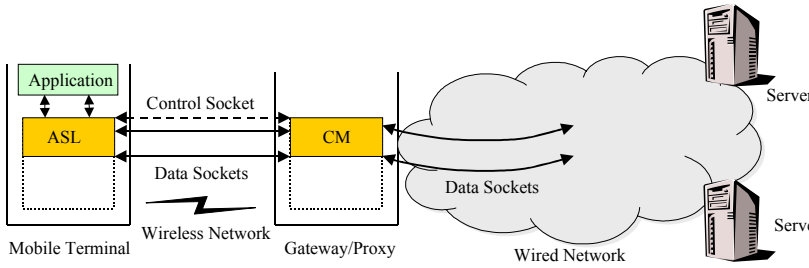

Fig. 2. ASL-CM Operation

ASL resides at the mobile terminal side and provides a socket-like Application Programming Interface (API). In this manner, every socket call initiated by a client application passes through the ASL library. ASL co-operates with the CM module, which is running at the Gateway/Proxy side, using a lightweight proprietary protocol, which operates over UDP (Control Socket). The purpose of this protocol is to have ASL and CM exchange control information that will enable them to manipulate (*OPEN*, *ReOPEN* and *CLOSE*) TCP connections, started by the terminal side. The CM module, upon receiving control messages, interprets them and tries to establish the required connections (Data Sockets) in order to realize the connection that the client application of the mobile terminal requested from ASL.

Figure 3 depicts the exchange of control messages, between ASL and CM, concerning the two most interesting situations. In the first case the application initiates a connection, through a TCP socket, with a server. The socket call is handled by ASL that establishes a connection with the application, registers the essential information of the connection, so as to be in position to duplicate it, and sends an *OPEN* message to CM, through the wireless medium. The CM module consecutively stores the required information that mirrors the connection information kept by ASL

and tries to connect both to ASL and the requested server. In case CM successfully establishes both connections, it returns an *Answer* message to ASL, indicating that the requested connection is active. In any other case the Answer message inform the ASL for the connection failure. Following the aforementioned procedure, the ASL and CM modules assemble an end-to-end connection between the application and the appropriate server.

In the second case, Figure 3 depicts the steps that ASL and CM follow to reopen a broken, due to the wireless medium properties, physical connection. ASL sends a *ReOPEN* message to CM, identifying the connection that must be reopened. CM compiles the *ReOPEN* message, retrieves the connection properties from its database, and re-establishes the required connection with ASL. Afterwards, it sends and *Answer* message to ASL, acknowledging the successful reconnection.

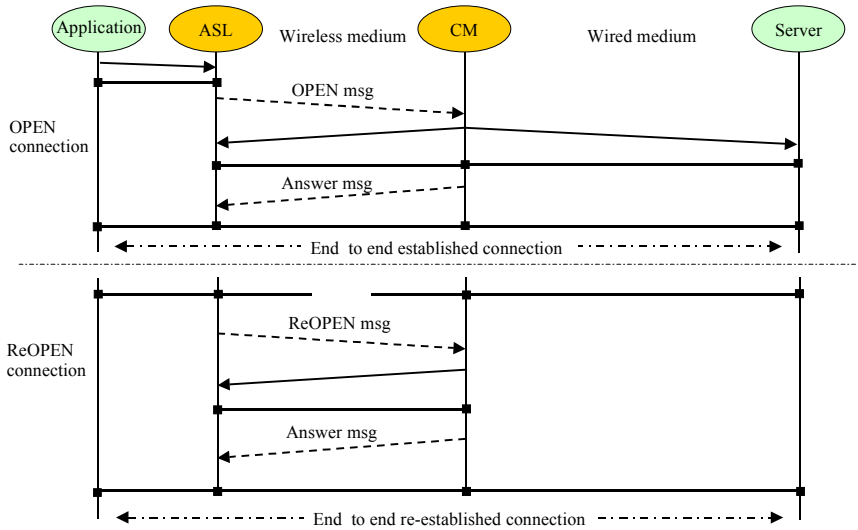

Fig. 3. Exchange of ASL – CM control messages

Splitting the original end-to-end connection between the client and the server application, into three parts (Application-ASL, ASL-CM and CM-Server) isolates the end points from the temporal wireless link disconnections. Whenever an interruption occurs, ASL re-establishes transport connections to CM, and, subsequently, re-associates sessions with physical connections. The terminal's networking applications throughout this period are "frozen", but not terminated.

In order for the aforementioned modules to communicate and co-operate properly, an additional mechanism is introduced in the terminal, called the Supervisor module [4], [5]. It is responsible for monitoring the connectivity status of the underlying wireless/wireline physical interfaces and selecting the most appropriate among them. The selection process takes place according to predefined signal strength thresholds and user preferences.

Moreover, Supervisor maintains a repository of necessary information in the terminal (Resource Repository). There it stores all values related to the operation of the various modules in the terminal architecture that are needed to be communicated between them. For example, connectivity status, signal strength values, IP and MAC addresses are vital parameters for the terminal operation. These parameters are supervised for changes and, in case of that, appropriate notifications to the interested modules are issued.

3. Reference Network Environment

The presented architecture is independent of the wireless interfaces. However, in order to validate its correctness, we have implemented a reference environment based on the two most widespread wireless interfaces in production: an 802.11-compatible wireless LAN (WLAN [6]) and GSM [7]. Alternatively to GSM, we have also tested access through a standard PSTN modem.

The mobile terminal is configured with the IPMEC, ASL, Supervisor and Resource Repository modules, and therefore it offers both location transparency and resilience to short disconnections. Its operation heavily depends on the selection of the underlying wireless medium.

When at home or office, the WLAN is always favored, as it provides more bandwidth than GSM, with low operational cost. On the other hand, WLAN coverage is quite limited. When the terminal moves towards the boundaries of the coverage area and the wireless LAN SNR (Signal to Noise Ratio) falls under a predefined threshold, the system switches to GSM. More particularly, it sets-up a GSM connection and registers the terminal to the Gateway/Proxy, in order to tunnel all terminal packets via the GSM. During the switching period, all running sessions are kept alive so that they are able to continue their operation after the new physical connection is established. A reverse switching is performed, when the WLAN signal rises to operational levels.

The Gateway/Proxy acts as bridge between the wireless and wireline parts of the corporate network. Additionally, the Gateway/Proxy is used to interconnect different sub-segments of the corporate network. It is configured with the IPMES and CM modules of the proposed architecture and manages a pool of modems that can be used to offer access through the GSM/PSTN network.

For the realization of the reference network environment, we have concluded to the utilization of a notebook PC as a mobile terminal, supplied with the appropriate WLAN and GSM/PSTN adapters. A notebook appears to be the preferred solution for a nomadic user, as it gives the capability of preserving a working environment, while moving between different locations. Knowing that the big majority of end-users are familiar with the Microsoft Windows environment, we have selected Windows NT 4.0 as the Operating System (OS) of the terminal. Additionally, in order to prove the generality and implementation feasibility of the proposed architecture, a separate implementation on a UNIX environment (Linux OS) has been also followed. The selection of the OS has, to a large degree, influenced the materialization of the overall architecture, introducing limitations and problems that have not been foreseen.

The adopted Reference Network Environment (Fig. 4) can support four different connectivity scenarios for accessing the corporate network, including indoor (WLAN) and outdoor (GSM/PSTN) access. More particularly:

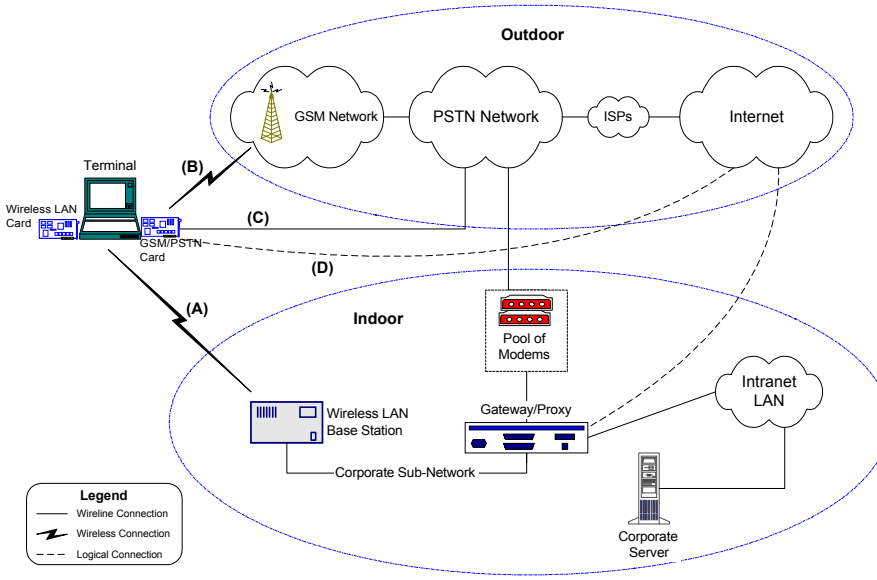

Fig. 4. Reference Network Environment

(A) The mobile terminal is located in the network segment in which its IP address belongs to and access is achieved by means of the WLAN interface.
(B) The terminal is connected to the corporate LAN utilizing a GSM physical link to the GSM service provider. At the GSM service provider's local exchange, traffic is routed, via a direct PSTN connection, to a modem pool, which is managed by the corporate Gateway/Proxy.
(C) The physical connection is achieved through the PSTN network only. In this case mobility is restricted, as the terminal uses a telephone line to connect to the corporate network. However, it may have lower cost, compared with scenario "B".
(D) A logical connection to the Internet is established utilizing the services of an Internet Service Provider (ISP). The physical link of the connection is achieved through the GSM or the PSTN interface. This scenario is quite close to cases "B" and "C". The main difference is that in scenario "D", an ISP router comes in between the terminal and the corporate Gateway/Proxy.

4. Trials and Results

In order to be able to test the implementation of the proposed architecture, a testbed has been established in the lab, but also a few trials have been performed in actual corporate environments. The testbed, following the Reference Network Environment, consists of the components listed below:

- *Mobile Terminal*: it is a notebook that uses Windows NT 4.0 OS and is configured with all the modules that our architecture proposes. Alternatively, we also used a notebook with Linux OS installed.
- *Gateway/Proxy*: it is a PC with Linux OS that is connected to corporate LAN. It is configured with the IPMES and the CM modules that are required from the architecture. Additionally, it serves as a dial-up server for the incoming calls from the mobile terminals.
- *WLAN Base Station*: it is the base station for the wireless LAN. It is connected to the same sub-network with the Gateway/Proxy.

The testing scenarios were based on standard networking applications, including Telnet and Web browsing (Internet Explorer for Windows NT and Netscape for Linux) and videoconference application (Microsoft NetMeeting for Windows NT). Additionally, a custom-built FTP-like application that utilizes directly the ASL library was used in the Windows NT environment. The use of this application separated the testing of ASL-CM pair of modules from the OS inherent restrictions. The testing scenarios that were used are described beneath (Fig. 5):

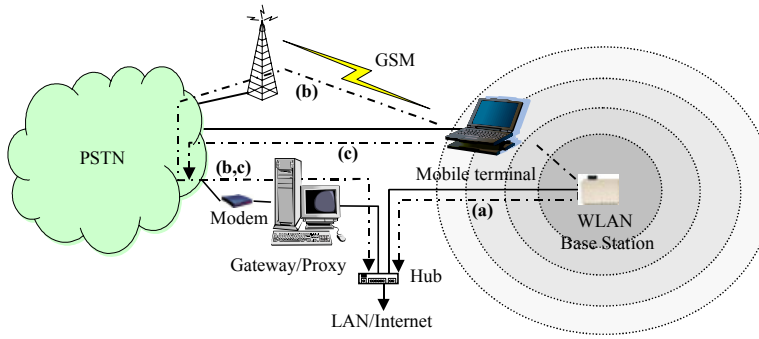

Fig. 5. Testbed Infrastructure

Scenario A: The mobile terminal is connected to the network through path (a). The selected networking applications are executed and operate normally. At this point, an automatic transition from WLAN to GSM link is performed, due to a deliberate degradation of the WLAN SNR. After the switching, network traffic is routed through the path (b). Alternatively, the PSTN dial-up connection, path (c), can be utilized. The desired result for the running applications is a seamless handover.

Scenario B: It is the same with scenario A, only this time the reverse transition from the GSM link to the WLAN is performed (from path (b) or (c) to (a)), due to an

increase of the WLAN SNR. The uninterrupted operation of the selected networking applications is the desired result.

Both scenarios have been tested for the cases where the mobile terminal was configured with the Windows NT OS and the Linux OS. In the former case, regarding scenario A, all the applications continue their normal operation unhindered. However, during the handover of scenario B, the telnet and videoconference applications fail to retain their connections. On the contrary, the custom application continues its normal operation and completes the file download. Additionally, the browsing application also continues its operation seamlessly.

The results with the Windows NT OS have strengthened the necessity to develop the ASL-CM pair due to the following reason. It has been observed that during switching from GSM to WLAN, TCP connections are lost, which did not occur in any of the experiments in the Linux OS. More particularly, while the terminal is operating over GSM (or PSTN) the Point-to-Point protocol (PPP [8]) is utilized. As soon as the Windows NT OS senses that the GSM link is down, it releases all resources related to the PPP protocol, with the imminent result of terminating any previously active TCP connection. Incorporating the ASL-CM pair solves this drawback.

In the case that the mobile terminal operates under the Linux OS, two representative networking applications were used: a common telnet application and the Netscape browser. The results, after applying scenarios A and B, are that both applications continue their operation unhindered, even if the switching of media occurred, while downloading an image (browsing).

According to the presented results, we see that switching between media, while maintaining the sessions at both the TCP/UDP and IP levels, occurs successfully in almost all examples, apart from the cases that are restricted by the operating system's limitations. Moreover, some performance measurements that have been performed during the execution of the testing scenarios, reveal that the time to setup a GSM connection can be very large, as it is about 20 seconds on average. This big duration can also result in the termination of existing TCP connections (due to time-out), in which case the existence of the ASL-CM pair provides a good solution for the applications that can make use of the socket-like API it offers.

Regarding the ASL-CM operation, some performance measurements have been executed using of the proprietary file transfer application. The average measured time to initially setup the end-to-end communication over the ASL and CM modules is 0.463 seconds, instead of the measured 0.152 seconds without the use of ASL-CM.

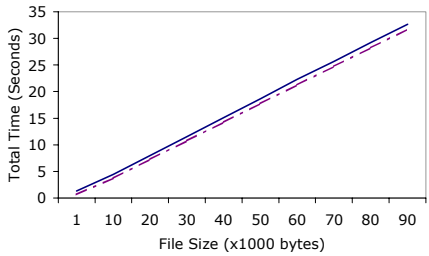

Fig. 6. Total Time needed to transfer files of various sizes with and without (dotted line) the use of the ASL-CM pair

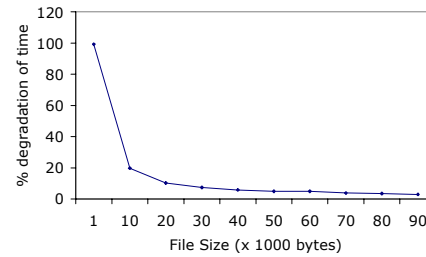

Fig. 7. The percentage of the degradation of the total time needed to transfer a file with ASL-CM compared to the case that the file is transferred without the ASL-CM pair

It has also been detected a degradation on the communication speed even when no interruption occurs (Fig. 6), especially for files that are small in size. Nevertheless, the degradation is decreasing very quickly to accepted values (Fig. 7). For example, for files larger than 20 Kbytes the degradation percentage is less than 10%.

In case of a disconnection, the application is frozen for as long as the physical connection is re-established and the ASL-CM pair re-associates sessions with TCP connections. The time for the former operation can be very large (20 seconds as mentioned above), while the average measured time for the latter operation is about 0.3 seconds. In this sense, the degradation is mostly owned to the establishment of the physical connection.

5. Conclusions

The architecture presented in this paper provides enhancements, both in the terminal and the Gateway/Proxy side, in order to support seamless and uninterrupted interworking between wireless and wireline interfaces. As a consequent, the end-user is not aware of the adjustments performed for the correct interworking of the underlying mediums.

The proposed architecture has been implemented under two different Operating Systems (Windows NT and Linux). Extensive experiments have been performed with standard networking applications and proved the correctness of the solution. In order to alleviate limitations posed by the OS, further enhancements (ASL/CM) are required for the case of Windows NT.

In addition to the functionality described in the paper, the architecture could be extended to various directions. To start with, although the implementation involves two specific wireless technologies, namely WLAN and GSM, it can be extended to include others, like the General Packet Radio System (GPRS [9]), which is the packet-based equivalent of GSM. Since the overall architecture is built in a modular manner, it can easily accommodate other wireless interfaces that fit better with the specific user needs.

Another extension, stemming from the ASL-CM pair, would be the encryption of the packet's contents before transmitting it to the CM and vice versa. This would apply a supplementary level of security over the security inherent in the WLAN or GSM radio transmission path. The charge for this is the probable degradation of transmission speed and delay, according to the selected encryption and decryption algorithm.

Acknowledgement

This work was performed in the framework of NOTE (NOmadic Teleworking business Environment - EP27002 [10]) project, co-funded by the European Community under the ESPRIT Programme. The authors wish to express their gratitude to the other members of the NOTE Consortium (Thomson CSF, Lucent Technologies NL, Archetypon, Solinet GmbH, Intrasoft International and Nationale Nederlanden) for valuable discussions.

References

1. C. Perkins, “IP Mobility Support”, RFC 2002, October 1996.
2. D. Plummer, “An Ethernet Address Resolution Protocol: Or Converting Network Protocol Addresses to 48.bit Ethernet Addresses for Transmission on Ethernet Hardware”, RFC 826, November 1982.
3. W. Richard Stevens, “TCP/IP Illustrated, Volume 1: The Protocols”, Addison-Wesley, Reading, Massachusetts, 1994.
4. S. Maniatis, I.S. Venieris, R. Foka, “Nomadic Teleworking Business Environment”, EMMSEC99, Stockholm, Sweden, Jun. 1999
5. K. Vaxevanakis, S. Maniatis, T. Zahariadis, N. Nikolaou, I.S. Venieris, N.A. Zervos, “A Software Toolkit For Providing Uninterrupted Connectivity Over a Variety of Wireless Physical Interfaces”, SoftCom99, Croatia & Italy, Oct. 1999.
6. IEEE 802.11 - Working Group for Wireless Local Area Networks, URL: http://grouper.ieee.org/groups/802/11/index.html.
7. ETSI, “General Packet Radio Service, GSM specification 03.60, version 6.2.0”, Oct. 1998.
8. W. Simpson, “The Point-to-Point Protocol (PPP) for the Transmission of Multi-protocol Datagrams over Point-to-Point Links”, RFC 1331 May 1992.
9. ETSI, “General Packet Radio Service, GSM specification 03.60, version 6.2.0”, October 1998.
10. ESPRIT NOTE – “NOmadic Teleworking business Environment, EP27002”, URL: http://www.telecom.ntua.gr/note.