Proceedings of the 4th WSEAS Int. Conf. on Information Security, Communications and Computers, Tenerife, Spain, December 16-18, 2005 (pp111-117)

Secure - Personal and Wireless Communications Systems

PEDRO PERIS, ESTHER PALOMAR, BELEN RUIZ, ARTURO RIBAGORDA
Department of Computing Science
Carlos III University
Avenida de la Universidad 30, 28911 Leganés (Madrid)
SPAIN

Abstract: - We are nowadays immersed in a great number of networks that permit us to have access to the information systems. Although it is a reality, there is a lack of interoperability between different networks, which would allow us a more universal access to the information systems. This paper presents an hybrid network architecture in order to achieve the integration of the personal communication systems and wireless networks, which we have called S-PWCS.

Key-Words: - Personal communication system, wireless communications, secure - personal wireless communications system (S-PWCS).

1 Introduction

The Wireless Technology is considered day by day more indispensable within the enterprise scope. Any enterprise needs the flexibility and cost savings the wireless lines offer for frequent changes.

Not only do they find application in the enterprises, but they also spread to public environments, airports, universities and hotels, to metropolitan areas, hospitals, congresses, and cafés, as a means of access to Internet or to support high user density areas (hot spots) in the close third generation networks (3G) [10].

In other words, a new corporative necessity has arisen that must be supported by a responsibility as a Information Technology Plan.

This paper presents the view of an hybrid architecture of efficient wireless access, orientated to the small and medium enterprise [1, 2]. For this aim, in the second section the different architectures of wireless network are checked that support the proposed model, which is shown in the third section. The previous sections study the initial problems that shown up in the wireless systems' incursion within the enterprise scope and how these services are supported.

Next, we discover the advantages and disadvantages associated with this kind of technology, and we will do a short journey of the technology, services and market's evolution.

1.1 Advantages and Disadvantages of Wireless Technology

Among the new possibilities the wireless networks offer, we find the ubiquitous communication, the broadband and a more advanced communication, the new services such as information integrity, information's typology and mobility, the connection systems for doing maintenances. They are all new possibilities that add to the already known ones, such as the possibility of allowing an easy incorporation of new users to the network, offer a low cost alternative to the wired systems, as well as accessing to any database or any application located within the network.

With the 3G technology, the total mobility and mobile efficiency arrive [11, 17]. The business moves wherever a worker is. We therefore stand out the following benefits: mobility, flexibility, relocation (without modifying the network's wiring), greater life time, smaller installation costs, resistance to external interference, easy maintenance and error detection, scalability and transparency for the user.

Any way, not all businesses can make the maximum profit of these kinds of information systems. But surely the most serious drawback of all is the security. Some security matters are the authentication, the integrity and the confidentiality, which will be dealt in the third section.

1.2 Evolution, Services and Market of Wireless Technology

The information systems have evolved regarding two dimensions, the location's independency and the flexibility of resources' use. High Speed Computer Networks, LANs, WANs and mobile computation appear in the early 80s. There has been an increase in the necessity of mobile phone services.

Some reasons of this grow are the bigger manufacture of wireless equipment, the IEEE 802.11 regulation, the interoperability consolidated on a stable platform and the costs' reduction [7, 9]. Many device manufacturers are introducing applications supported by wireless communications [6].

The worldwide wireless networks' evolution is basic for the proliferation of the wireless services that has ranged more than 1.600 million worldwide subscribers. For 2006 is expected, according to EITO, to range 1811 million users [5].

Depending on the type of service, wireless services market can be divided up into: text, Internet, compressed video and digital video, and the real throughput, as we illustrate in Fig.1. The 3G's purpose is the voice and data's convergence with wireless access to Internet, multimedia application and high data transmission.

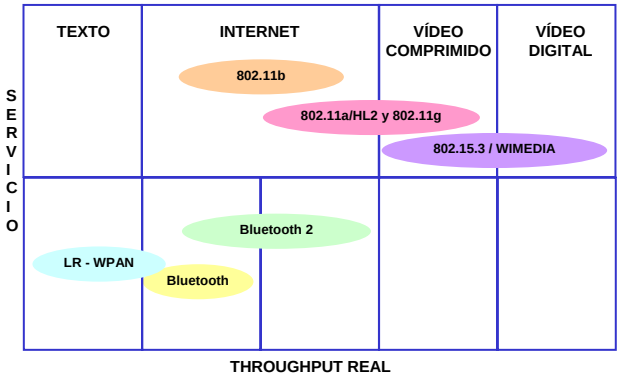

Fig.1 Wireless network's market.

1.3 Initial Problems of Wireless Technology

Initially, the lack of standards forced the different manufacturers to develop their own solutions, and intrinsically businesses were forced to adopt certain platforms with limitations concerning interoperability and compatibility.

Services' availability was a type of limitation too, as the wireless networks at that moment only supported data services.

Regarding security, even still the users are reluctant to the use of e-commerce applications through mobile devices, due to the lack of appropriate attention.

2 Architecture

When we talk about personal communication system (PCS) we refer to a variety of personal mobile systems and wireless accesses provided through a small dimension terminal, with the main aim of allowing communications anywhere, any moment and any way [3, 4].

2.1 Personal Communication Service

The PCS systems' technology has quickly grown in the telecommunication industry. The two most important areas are: cellular telephone system and wireless systems of medium and short range. The architectures of these types of technologies (Fig.2) are very similar, mainly consisting of two parts:

a. Radio network: the PCS users use mobile stations (MSs) to communicate with base stations. We can consider as mobile station a mobile phone, a laptop, a PDA…

The range's radius of the base station or station base's sector is called cell. In systems such as GSM, CdmaOne, and PACS, the station base is divided in two parts, the controller and the radio transmitters/receivers [14]. The base stations will be connected with the transport network wired, for this they will use a terrestrial link or a dedicated microwave link.

b. Transport network wired: the mobile switching centre (MSC) connects the base station with a special switching for mobile networks. The MSC is connected to the public switched telephone network (PSTN) to have service with this type of users. The MSC is also connected with one or various databases to draw localizations of the mobile stations, obtain data of the subscribers, etc.

In the last 20 years, a big number of PCS systems have appeared due to the strong market's demand. Some long-range cellular systems (mobile phone systems) are: GSM, DAMPS, PDC and CdmaOne [12, 13].

Further, among the standard short range communication systems for residential use, business use and wireless access applications are: CT2, DECT, PACS and PHS.

Finally, we would have to include the broadband wireless systems that would allow us to incorporate to the mobile systems both Internet and other multimedia services that require a big broadband. Some examples of these systems are the following: Cdma2000, W-CDMA and SCDMA [15, 16, 17].

2.2 Wireless Communications

Within the wireless networks there is a great variety of technologies. A possible classification can be made according to its range: WPAN, WLAN, and WMAN.

The WMAN networks are point to multipoint networks, designed for the Internet access and substitution of the local loop. Some examples can be LMDS or MMDS protocols, etc.

2.2.1 Wireless Local Area Networks

They cover a distance of some hundred meters. These networks are thought to create a local area network

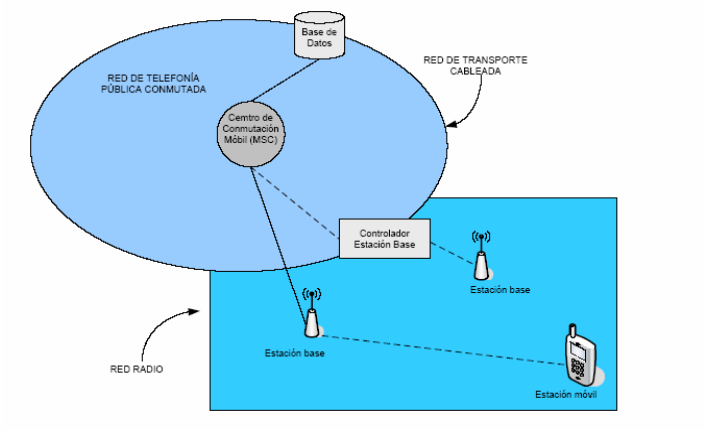

Fig.2 PCS Architecture.

between computers or terminals situated in a same building or group of buildings. There are different kinds of technologies; the most important are the 802.11 family, HyperLAN (supported by ETSI) and the HomeRF (thought for communications between home devices). Of all these technologies, it is possible to think that for 2010 there will be only one standard for the WLAN. However, nowadays, among the technologies mentioned before, 802.11 protocol is the most used in its different versions [7, 9].

The most basic configuration is the so-called from equal to equal or ad-hoc (Fig.3) and it consists of a network with two terminals connected through the wireless card, and each of them must be in the coverage area of the other one.

In order to increase the previous configuration's range, there is the infrastructure configuration. It consists of two elements: the access point and the client's devices. The access points (AP) act as a switching, receives and sends information via radio to the client's devices. The client devices can be of any type, usually PC, PDA, etc. With the access point's use we have achieved an increase of the range, the maximum distance permitted now is not between two stations, but between each station and access point. Moreover, the access points can be connected to other networks and in particular to a fixed network. In order to give range in a specific area, various access points will have to be installed.

Once this introduction is accomplished, let's focus on the 802.11 protocol. The original forecast (1997) of 802.11 foresaw connections of 1 or 2 Mbits/s in the 2,4GHZ band using two types of technologies: Frequency-Hopping Spread Spectrum (FHSS) and Direct Sequence Spectrum (DSS).

After the original 802.11 standard, other standards have come out (802.11 b/g/a) getting speeds up to 54Mbits/s. These new standards achieve a bigger transmission measure thanks to more efficient use of

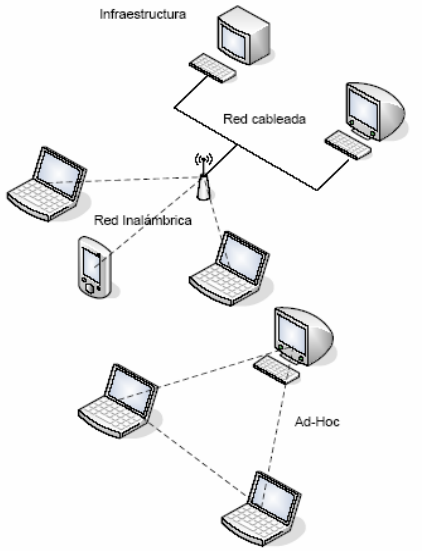

Fig.3 Wireless Networks Configurations

modulation techniques, for example, OFDM. The first two 802.11 b/g continue operating to the frequency of 2,4GHz, whereas the latter operates to the frequency of 5GHz.

2.2.2 Personal Local Area Networks

They cover a distance of 10 metres. Among these technologies stand out the technologies such as Bluetooth, Zigbee, IEEE 802.15, infrareds, etc [8].

The most used is Bluetooth though its scope degree is much lower to the expected one. The low penetration of these devices is because of the circuits' cost.

The Bluetooth specification defines a maximum communication channel of 750 kb/s with an optimum range of 10 metres, they operate in the work frequency of 2,4 GHz and they use a FH/TDD modulation (frequency hopping/ time duplex division).

3 Secure - Personal and Wireless Communications Systems

Throughout the previous two sections we have made a brief explanation of the main communication services that can be found in an information system. However, we can go further in the development of these technologies achieving a bigger interoperation between the PCSs systems and the wireless networks.

For this aim, a new architecture is proposed that will be called S-PWCS (Secure – Personal and Wireless Communications Systems). It is an hybrid architecture, achieving both system's integration, without forgetting one of the main aspects of the communications that is security. For this, firstly we will introduce the S-PWCS network's architecture and next we will explain the security measures proposed.

3.1 S-PWCS Architecture

The S-PWCS system is made up of a PCS network and a wireless network. Fig.4 illustrated the scheme of the hybrid architecture proposed.

As we can see in the previous figure, the PCS networks and the wireless networks are linked throughout an element called Gateway, a device that carries out the protocol's conversion between different types of networks. This element will be divided in two parts:

a. NET- Gateway: it acts as an intermediate between the data networks (IP) and the mobile phone networks. The proposed solution provides an interface between the PCSs networks and the wireless networks (IP). It will facilitate an access from the terminals (IP) to the mobile voice services supported up to now mainly within the PCS networks. It will be in charge of the signaling functions, implemented by means of some protocol, for example SS7.

b. WAP-Gateway: it acts as an intermediary connecting on the one hand the mobile phone network and on the other hand Internet and/or the corporative intranet. It provides a wireless access to Internet from the mobile stations (MS) of the PCSs networks. A proxy carries out the server's and client's functions, making requests on behalf of the client. The MS will use a WAP navigator in its mobile terminal to connect to the WWW or WAP server where the applications we want to have access are.

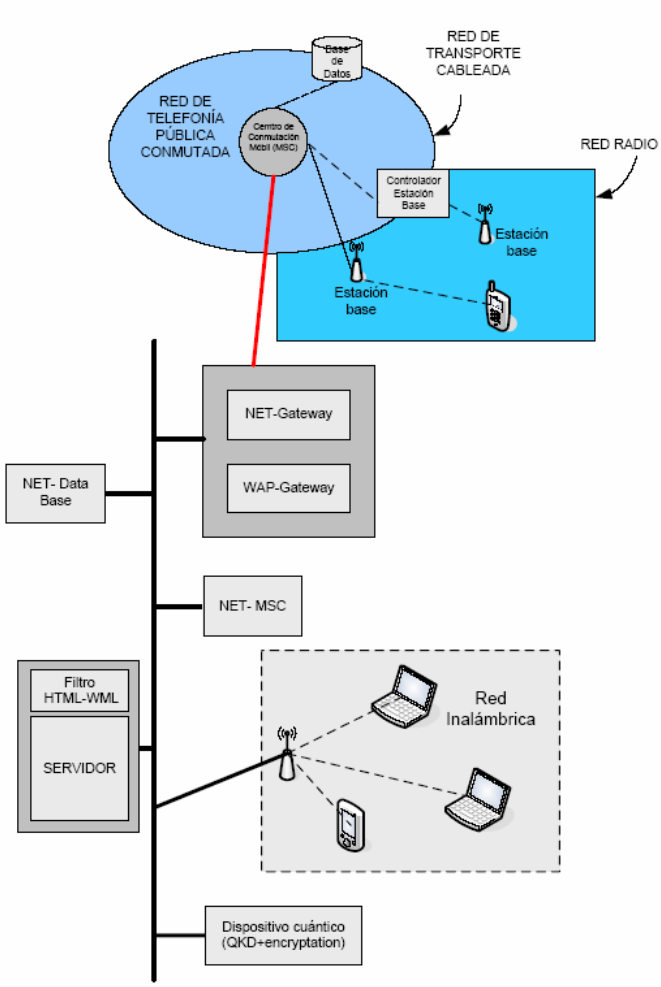

Fig.4 S-PWCS network's architecture.

Only with the Gateway we dispose of a joint interface between these two networks, so it is necessary to introduce some more elements. The main element of this architecture will be an "IP-PCSs switching central", which has been called Net-MSC. This "switching central", as the PCS network's switching central, will have for main aim the call's management. In order to carry out this management in an efficient way, it is necessary to maintain an information repository of all the users subscribed to the system. We have therefore added a database that has been called Net-Date Base. Finally, we have included in the architecture a web-server. This web-server has been incorporated a HTML-WML filter to be able to respond to the requests from the MS via WAP.

Next, the main functions of these elements are detailed as follows:

a. Net-DataBase: it contains all the administrative information about the service's client and the current terminal's location. Through the Net-DataBase the network verifies whether a wireless terminal (IP) has authorization to use the service. If the answer is affirmative, then the Net-MSC will send an authorization message to the terminal. The information kept in this database will be the following:

- Subscription Information (payment information.)
- IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Station International ISDN Number.)
- Location Information.
- Subscription Information of the different teleservices and bearer services.
- Information of supplementary services.
- Services' restrictions.

b. Net-MSC: It is the network's centre through whom the "switching" of a call made from a wireless terminal (IP) to a mobile terminal within the PCS network is performed. Specifically, it develops the following management functions:

- Call management functions: establishment and liberation, routing.
- Mobility management functions: location, authentication.

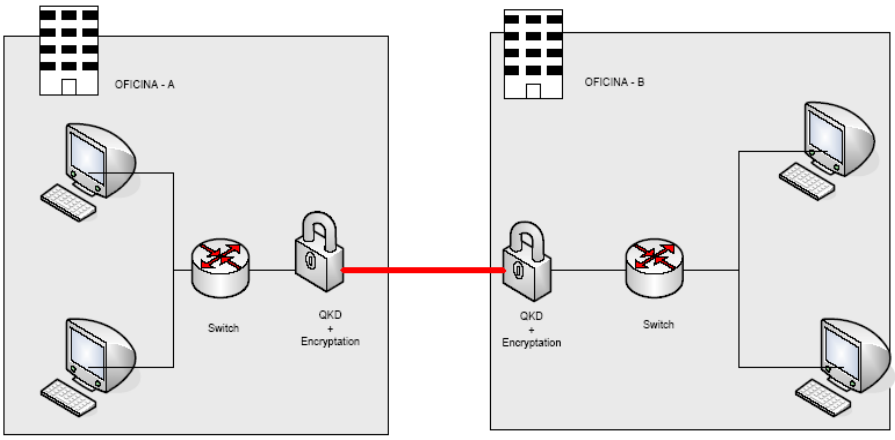

Fig.5 Quantic Key Distribution

c. Server: the server will be composed of two elements. The first one will be the web-server strictly speaking; it would be implemented for example by Apache. The second element would be the HTML-WML filter that will adapt the requests provided by the web-server so that they can be shown in the mobile stations (MS) despite its restrictions, for example, its limitations of the screen's size.

Inside the wireless network defined in the previous section, we include the following elements:

a. IP/PHONE (H323). The IP telephonic devices will use the ITU-T H.323 protocol [18, 19]. This protocol allows us to carry out multimedia communications throughout networks of packets' switching, which do not provide a guaranteed service quality. Therefore the mobile devices of the wireless networks will implement this protocol and, as we have seen, will access to the data networks through the access points (AP). The communications will be accomplished under Net-MSC's supervision for which the terminals or users will be authenticated.

b. Radius- Server (Remote Authentication Dial-In User Service) is a widely used protocol, which provides authentication and authorization centralized for access to all kind of networks. It is a concept introduced in the 802.11x protocol whose function will be explained in the following section.

3.2 S-PWCS Security Aspects

In the previous section, we have made a description of how the integration of the PCS's networks and wireless networks could be done. One of the most important aspects and that we have not taken into account up to now, is the security in the S-PWCS networks. We have to make the following considerations about the security:

a. In the case of the wireless devices, it is not recommended to make use of WEP owing to the vulnerabilities it presents. For people who are not familiarized with this technology, remember that the main characteristics of these systems regarding security are the following: RC4 (40 bits), generation of static keys and distribution of manual keys. Because of known vulnerabilities of these systems, we recommend the use of WEPA. For the use of this technology, it is necessary to introduce, as well as the access points, the radius sever(s) that allow the clients to authenticate with the server. To accomplish this authentication, we suggest the mode EAP-TLS be used, for which it will be necessary that both the server and the clients have a certificate. Although it's true that the public key's infrastructure (PKI) is still not totally spread, we believe this would be the optimum way to guarantee the security. Once the server and the client have authenticated, they will agree the used session key; this is one of the strengths of these type of systems, that the key is actualized in a dynamic way. Although this section does not aim to explain deeply these kinds of systems, we summarize briefly the characteristics of these systems for those who are not familiarized with them: TKIP-RC4 (128 bits), dynamic key management (by user, by session and by packet) and automatic key distribution managed by 802.11x/EAP.

b. In the case of devices that implement the H.323 protocol, for example, an IP telephone, the RAS protocol will be used (register, admission and state). In order to guarantee the authentication and integrity, MAC function (message authentication code) will be used, particularly a HMAC-SHA1-96 function. In order to guarantee the confidentiality, the protocol uses the RC4 or DES by default, it is recommended the use of a stronger code for example AES of 192 bits. One of the problems we can come across in these systems is the lack of specification of the key management; ideally, we would be to carry out a key management in a dynamic way.

c. Finally, as we have reference in various occasions, one of the most relevant aspects and one of the problems which come across when work with cryptographic security protocols is the key's

distribution. To solve this problem, we propose the quantum cryptography [20, 21, 22] be used, which is a reality since a very short time, and it already exists in commercial devices, although its price is still high. We therefore suggest using this technology only for the connection of two data networks, for example, two networks belonging to a same enterprise situated in different places of a city, as it is shown in Fig.5.

For this aim, these two networks will be linked by means of a fiber optics' wire, being 100km the maximum distance between these two networks. In each end of both networks, we have to place a QKD, which can be seen simply as a network device of level 2. The advantage of using this technology is that it allows, as some of its manufacturers specify, a key actualization speed up to 100 times per second.

Finally, we have to remind people that are not familiarized with quantum cryptography [26, 27, 28], which the security of these systems lies in the following quantum physics' principles:

- The no cloning theorem ensures that a quantum state $\psi\rangle$ can not be copied.
- The quantum measurements are irreversible.
- Any attempt to obtain information about a quantum system entails a certain modification of it.

3.3 Advantages of the Proposed Architecture

We have studied a hybrid network's scheme between the PCSs networks and the IP networks – in particular the wireless networks, although it could be extrapolated to the wired networks. There are many advantages of this proposed solution:

a. Interoperability: thanks to the proposed network architecture, it is allowed the interoperability of the mobile communication networks with the wireless data networks (IP). In order to guarantee the interoperability in both directions, we have included as a WAP gateway as a network gateway, Net-Gateway. Through the WAP gateway we allow the access to the MS' data networks, and through the network gateway we allow the network's wireless terminals have access to the services provided by the PCSs networks, for example voice services.

b. "Universal" access: One of the aims always pursue in telecommunications, is to allow through a same device the access to the largest possible number of services. We can take for instance the PDAs example, which have appeared recently in the market, with connectivity to wireless networks, Bluetooth, GSM/GPRS. However, although it is true that these devices allow us to have access to different networks, they do it in an independent way. In the proposed architecture, we pretend by the inclusion of a reduced number of elements, to have access from the wireless networks to the PCSs networks and vice versa, achieving a more "universal" access to the telecommunication services.

c. Scalability: the suggested architecture is not a rigid architecture; on the contrary, it is totally scalable depending on the number of users. Figure 4, for example, shows an only one Net-MSC but more than one will exist depending on the number of users that are in the network. The network is flexible and can cope with the number of users that demand its services. This will make that the implement of the network's infrastructure will be possible to be made in a gradual way, without having to do a big investment for the initial operation of the necessary infrastructure.

d. Larger number of services: as a result of the access from the data networks (IP) to the PCS networks, it affords the networks operators the opportunity of new services appearance, which could be used not only by the wireless devices (IP) but also by the MS devices of the PCS networks. The inclusion of these new services will give a greater value of these types of networks.

e. Moderate costs: on account of the number of network's elements introduced not being very large, and thanks to the proposed architecture's scalability, the implement of the following architecture will mean moderate costs, compared to the benefits it will entail.

4 Conclusion

One of the problems we usually come across when working with communication networks, understanding by network any network "infrastructure" that allows us the communication between two devices, it is the lack of interoperability between the different networks in existence.

By means of the proposed network's architecture we achieve:

1. Adding a reduced number of elements, whose function has been explained, we achieve interoperability between the PCS networks and the wireless networks.

2. Not only is it important to ensure the network's interoperability, but it must be done it in a secure way. We have therefore put forward the use of WEPA, RAS (H.323) and QKD to link two data networks that are situated less than 100 km from each other. The quantum cryptography's use would provide great security to the communications, the quantum physics' principles already mentioned be reminded, allowing us to solve the key distribution's problem and its actualization in a dynamic way (up to 100 times per second).

3. Thus, the presented hybrid architecture, S-PWCS, would be of great utility since it would allow us to have access from wireless networks to personal communication systems and vice versa, being accomplished in a totally secure way. All this with the benefits mentioned previously: "universal" access, scalability, larger number of services…

References:

[1] Kaveh Pahlavan, Wireless Information Network, John Wiley & Son, 1995.

[2] Kaveh Pahlavan, Principles of Wireless Networks: a Unified Approach, Prentice Hall PT, 2002.

[3] David J. Goodman, Wireless Personal Communications Systems, Prentice Hall PTR, 1997.

[4] Yi-Bing Lin, Wireless and Mobile Network Architectures, John Wiley & Son, 2001.

[5] Jyh-Cheng Chen, Tao Zhang, IP-Based Next-Generation Wireless Networks: Systems**,** John Wiley & Son, 2004.

[6] Rob Flickenger, Building Wireless Community Networks**,** O'Reill, 2002.

[7] IEEE, 802.11 Standards, available in http://grouper.ieee.org/groups/802/11/.

[8] IEEE, 802.15 Standards, available in http://www.ieee802.org/15/.

[9] Matthew S. Gast, 802.11 Wireless Networks: the Definitive Guide**,** O'Reill, 2002.

[10] Clint Smith, 3G Wireless Networks, McGraw-Hill, 2002.

[11] Timo Halonen, GSM, GPRS and EDGE performance: evolution towards 3G/UMTS, John Wiley & Son, 2002.

[12] Gunnar Heine, GSM Networks: Protocols, Terminology and Implementation, Artech House, 1999.

[13] José María Hernandez Rábanos, Comunicaciones Móviles: GSM, Fundación Airtel, 1999.

[14] Luis Arroyo Galán, Tecnología Móvil: GSM, GPRS, UMTS y WIFI, Anaya Multimedia, 2003.

[15] Harri Holoma, WCDMA for UMTS: Radio Access for Third Generation Mobile Communication, John Wiley & Son, 2002.

[16] Valtteri Niemi, UMTS Security, John Wiley & Son, 2003.

[17] Miguel Calvo Ramón, Sistemas de Comunicaciones Móviles de Tercera Generación IMT-2000, Fundación Airtel-Vodafone, 2002.

[18] Information available about H.323, http://www.h323forum.org.

[19] ITU, H.323 Standard, http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.323.

[20] C.H. Bennett and G. Brassard, Quantum Cryptography:"Public key distribution and coin tossing", Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (1984) 175-179.

[21] C.H. Bennett , Quantum Cryptography using any two nonorthogonalstates, Phys. Rev. Lett. 68 (1992) 3121-3124.

[22] D. Mayers, Unconditional Security in Quantum Cryptography, Submitted to Journal of ACM; arXiv:quant-ph/9802025 v4 (1998).

[23]Alfonsa García López; Jesús García López de Lacalle, Presentación en el Primer Congreso Conjunto de Matemáticas RSME-SCM-SEIO-SEMA, Universidad de Valencia, España, 31 de enero al 4 de febrero de2005.

[26] Quantum Cryptography Tutorial, available in http://www.cs.dartmouth.edu/ jford/crypto.html, (June 2005).

[27] Gilles Brassard, A Bibliography of Quantum Cryptography, Available at http://www.cs.mcgill.ca/ crepeau/CRYPTO/Biblio-QC.html, (Junio 2005).

[28] Centro de computación cuántica de Oxford, Available at http://www.qubit.org, (Junio 2005).