International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 4 Issue 2 May 2013

ISSUES OF INTEROPERABILITY AMONG HETEROGENEOUS WIRELESS COMMUNICATION NETWORKS

T. L. SINGAL

Professor, School of Electronics and Electrical Engineering

Chitkara University, Chandigarh

Abstract: - Several overlaid wireless networks such as 3G Cellular, Wireless LANs (WiFi), Wireless MANs (WiMAX), Mobile Adhoc Networks (MANETs), Wireless Mesh Networks (WMNs) and Wireless Sensor Networks (WSNs) may exist over the same geographical area. The requirement of interoperability among these heterogeneous wireless communication networks is of utmost importance. Spectrum conflict is the potential for competing technologies using the same frequency bands to interfere with each other to the extent that their performance degrades significantly when used within close operating range of each other. The interworking of these diverse wireless technologies for efficient delivery of value-added applications and services lead to several challenging issues, mainly related to architectures, resource allocations, mobility management, quality-of-service (QoS) provisioning, and security. The focus of this paper is to discuss various aspects of interoperability of heterogeneous wireless networks and to investigate how some of the serious concerns can be addressed. The emerging IEEE 802.21 standards which allow seamless and transparent handovers among different entities of heterogeneous wireless network are also discussed here. The user authentication and data security issues are other serious concerns for interoperability of heterogeneous wireless network. Many standards are currently emerging, and interoperability testing is needed to ensure reliable interoperability between different implementations.

Keywords: 4G, Handover, Interoperability, Heterogeneous Networks, Security, Spectrum Conflict

1 Introduction

Recent years have witnessed the rapid evolution of commercially available wireless mobile computing environments. Modern digital wireless networks and technologies support higher system capacity, provide superior voice quality and adequate data security. The user wireless device has the potential to become a generic platform for, or gateway to, the complete range of value-added communication services that include voice, data, video and multimedia. [1]. The existing digital wireless standards continue to be developed, particularly related to bandwidth, coverage, capacity, inter-working, value-added services, and, of course, costs. All major service providers of wireless network systems, services and user devices agree that next-generation heterogeneous wireless networks should evolve from the core infrastructures available in today’s digital wireless networks.

The next significant development in wireless networks will consist of enhancements to the radio access that enable true multimedia services to be delivered at high transmission bit rates. With the advancement in mobile information technologies such as user-controllable software defined radios, ultra high-speed transmission data rates, mobile Internet protocol MIPv6, the potential users would be able to access the Internet on the move; use cell phone or laptop computer or any other PDA as mobile communication device; choose freely the services, applications and service providing networks; and achieve advanced mobile E-commerce applications with higher levels of data security and integrity during data transactions. [2].

Wireless mobile communication networks (e.g. 3G and beyond) and broadband wireless data access solutions (e.g. WiFi and WiMAX) provide numerous applications and services ranging from voice calls to video streaming. The emerging user personalized requirement demands integration of different wireless access solutions into a single, unified, communications platform capable of delivering seamless and transparent user mobility with high level of Quality-of-Service (QoS) for the end users. This integration leads to the notion of Heterogeneous Wireless Networks (HWNs). One of the typical aspects of HWNs is the reconfigurable interoperability which requires management of different resources in heterogeneous environment. The increased level of users' demands and the integration of various wireless access networks leads to the development of a multi-access, heterogeneous, personalized and user transparent wireless communicating environment, i.e. 4G, as depicted in Fig. 1. [3].

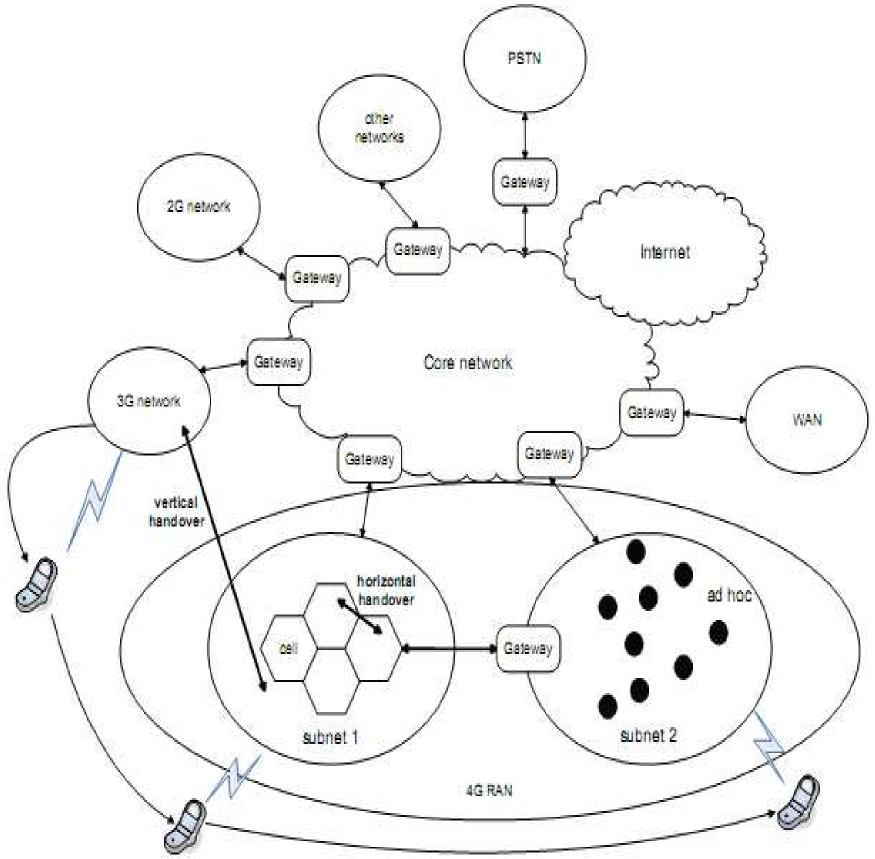

Fig. 1 A Typical Heterogeneous Wireless Network

The interoperability among different wireless networks requires novel resource management techniques. The heterogeneous environment poses serious challenges for the mechanisms responsible to accommodate the efficient networks usage as well as the users' satisfaction. The paper is organized as follows. Section 2 describes the notion of spectrum conflict among various wireless communication systems operating in Heterogeneous Wireless Networks. Section 3 reviews IEEE 802.21 standards which supports algorithms to enable seamless handover between heterogeneous wireless networks and allows for easier introduction of resource management schemes. Section 4 elaborates the security concerns along with some data encryption methods commonly used in wireless networks. Finally, section 5 concludes the paper, highlighting various aspects and serious concerns for reliable interoperability of heterogeneous wireless networks.

2 Spectrum Conflict

Of all the issues with wireless local area networks (WLANs) and wireless personal area networks (WPANs), spectrum conflict is potentially the most serious concern. Spectrum conflict, in general, is the potential for competing wireless networking technologies using the same frequency bands to interfere with each other. This may degrade their performance significantly when used within close operating radio range of each other. For example, IEEE 802.11b/g WLANs perform poorly in operating environments where a 2.4 GHz cordless phone is also in use nearby. This problem affects all DSSS and FHSS based wireless communication networking technologies operating in the same frequency band. To avoid the technical support issues related to spectrum conflict, manufacturers of cordless phones have started introducing models that operate in another unlicensed ISM 5.8 GHz band.

Bluetooth can conflict with other technologies such as IEEE 802.11b and 802.11g WLANs that also use the ISM 2.4 GHz band for transmission. Using Bluetooth and 802.11b/g WLAN devices in close proximity to each other may cause the WLAN to drop the connection if it detects that another device is sharing its frequency. One simple way to resolve this problem is to move the Bluetooth device away from the 802.11b/g device. It is also recommended in IEEE 802.15.1 standard that Bluetooth and 802.11b/g WLAN devices share the spectrum by first checking to see if the air medium is clear for transmission. [4]. The 802.11a WLAN standard uses a different frequency band which helps to avoid the spectrum conflict all together. The actual performance may vary when these products are deployed in large volume and in many different operating environments.

Likewise, applying Ultra Wide Band (UWB) technology to WPAN standards may considerably reduce the problem of spectrum conflict. For example, relatively wideband interference, such as that generated by IEEE 802.11b wireless networks, appears like white noise to an IEEE 802.15.4 low-rate WPAN receiver because only a fraction of the 802.11b power lies within the 802.15.4 receiver bandwidth. To an IEEE 802.11b receiver, the signal from an 802.15.4 transmitter appears like narrowband interference. In addition, the low duty cycles typical of ZigBee devices further reduce the impact of interference. [5]. Similarly the impact of interference from IEEE 802.15.1 Bluetooth devices should be minimal due to much smaller bandwidth of each frequency channel. And 802.15.4 devices should only interfere with approximately three out of the 79 frequency hops of a Bluetooth transmission, which is approximately 4% only.

UWB can interfere with IEEE 802.11a networks too. ZigBee and WiMedia products should be able to coexist with 802.11b/g without any serious problems. One of the concerns of end users and service providers when considering wireless data transmission in the unlicensed bands is that as the number of simultaneous transmissions increase, interference also increase in the same proportion. Eventually, this can make the technology unusable. It is of particular importance considering the distances achievable with IEEE 802.16 WiMAX technology. WiMAX is different from 802.11 technologies in that it is not limited to the 2.4 GHz or the 5 GHz bands. The ISM band offers approximately 80 MHz bandwidth whereas the U-NII band offers about 300 MHz bandwidth and 12 channels which can be shared by users and service providers. Depending on the distance between transmitters, interference may not be a serious problem since WiMAX signals are limited to approximately 48-56 kms under ideal line-of-sight conditions. Moreover with the use of adaptive modulations, variable data rates, and FEC, the concerns about interference can be easily resolved by testing the performance of a wireless communication link. The deployment of smart antenna systems is also another viable solution to this type of problem.

3 Handovers and Roaming

The evolution and the emerging variety of different wireless systems with different characteristics require integration into a single platform which is capable of supporting transparent and seamless user roaming through handovers without interrupting on-going communications. This process is followed by the development of new user devices designed to deal with the various network platforms and protocols. The implementation of HWNs is strongly facilitated by the lately emerging IEEE 802.21 standard [6]. This standard mainly aims to provide a Media Independent Handover Function (MIHF) to heterogeneous environments which allows seamless and transparent user roaming. The IEEE 802.21 standard enhances the user experience of mobile devices by supporting handovers between heterogeneous wireless networks. Moreover, the IEEE 802.21 standard allows for easier introduction of resource management schemes. Fig. 2 depicts IEEE 802.21 framework.

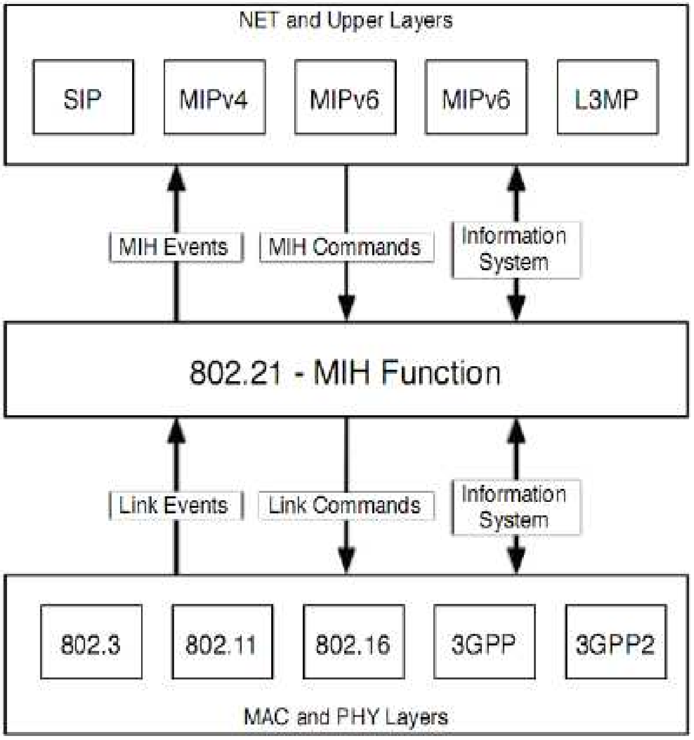

Fig. 2 IEEE 802.21 Framework

The IEEE 802.21 is an emerging wireless networking standard which supports algorithms to enable seamless handover between networks of the same type as well as handover between different network types. For example, the 802.21 standards provide information to allow handing over to and from cellular (2G/3G), IEEE 802.11 WLANs, WiFi, Bluetooth, and IEEE 802.16 WiMAX networks through different handover mechanisms. Digital cellular networks and IEEE 802.11 wireless networks employ handover mechanisms for handover within the same network type, termed as horizontal handover. Mobile IP provides handover mechanisms for handover across subnets of different types of networks, but can be slow in the process. The salient features of IEEE 802.21 standards include roaming between 3G cellular networks and IEEE 802.11 wireless networks, ad hoc teleconferencing, applicable to both wired and wireless networks, compatibility and conformance with other IEEE 802 standards, adaptability by multiple vendors and users. Although security algorithms and security protocols will not be defined in the standard, authentication, authorization, and network detection and selection will be supported by the protocol. Heterogeneous wireless networks encompass a variety of different wireless access solutions. Users should be able to move seamlessly and transparently in such an environment performing vertical handovers through different access technologies. IP mobility support for next generation heterogeneous mobile networks is shown in Fig. 3 [7]. The provision of authentication, authorization, and accounting (AAA) together with quality of service (QoS) control, are also provided.

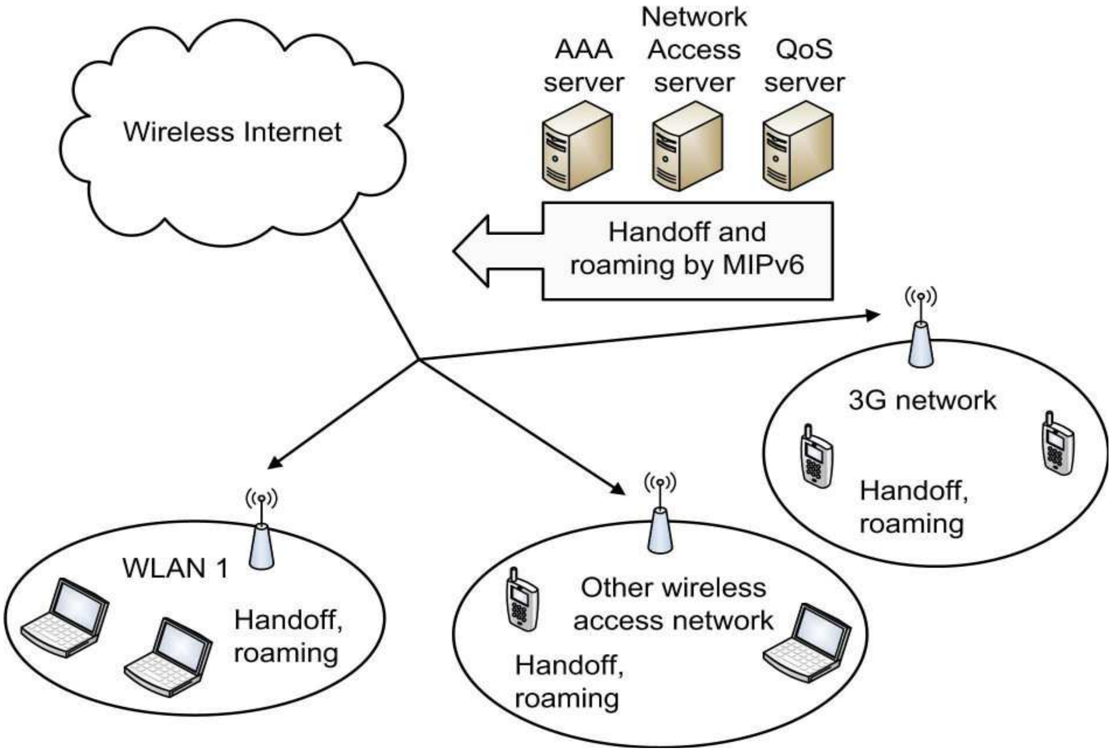

Fig. 3 Mobile IP Support in HWNs

Vertical handover refers to a network node changing the type of connectivity it uses to access a supporting infrastructure, usually to support node mobility. The vertical handovers in heterogeneous environments depended heavily on pure Mobile IP [8] functionalities leading to high handover latencies and disconnection times, and high number of dropped packets. For example, a well-equipped laptop might be able to use both a high speed wireless LAN and a cellular network for Internet access. Wireless LAN connections generally provide higher speeds, while cellular technologies generally provide more ubiquitous coverage. Thus, the laptop user might want to use a wireless LAN connection whenever one is available, and to switch over to a cellular connection when the wireless LAN is not available. Vertical handovers also refer to the automatic switchover from one technology to another in order to maintain communication link. This is different from a horizontal handover between different wireless access points that use the same technology in that a vertical handover involves changing the data link layer technology used to access the network. Vertical handovers among a range of wired and wireless access technologies including WiMAX can be achieved using media independent handover functions (MIHF). MIHF enables the handover of IP sessions from one layer to access technology to another layer, to achieve mobility of end user devices. The importance of MIHF derives from the fact that a diverse range of broadband wireless access technologies is available and in course of development, including GSM, UMTS, CDMA2000, WiFi, WiMAX, Mobile-Fi and WPANs. Multimode wireless devices that incorporate more than one of these wireless interfaces require the ability to switch among themselves during the course of an IP session, and devices such as laptops with Ethernet and wireless interfaces need to switch similarly between wired and wireless access.

When a session is handed over from one access point to another access point using the same technology, the handover can usually be performed within that wireless technology itself, even without involving IP or MIH functionality. For instance, a voice over internet protocol (VoIP) call from a WiFi handset to a WiFi access point can be handed over to another WiFi access point within the same corporate network using WiFi standards such as IEEE 802.11f and IEEE 802.11r. However if the handover is from a WiFi access point in a corporate network to a public WiFi hotspot, then MIH is required, since the two access points cannot communicate with each other at the link layer, and are in general on different IP subnets. When a session is handed over from one wireless technology to another, MIHF can provide the handover by passing messages among the wireless technologies and IP.

4 Security Concerns

A lack of effective security standards has slowed down the business adoption of WiFi networks. The combination of an essentially useless security protocol implemented on loose access points creates a huge potential security hole in any business infrastructure. While the unauthorized entry to conventional wired LANs can be blocked by deploying firewalls and taking other measures at specific locations, WiFi networks offer access to anyone who can get physically close enough to the access point. Since WiFi is the dominant wireless networking technology at the moment, with a high promise to provide seamless mobility among current subscribers as well as future potential users, authentication and data security issues, other than high-speed reliable data transmission service, remain the main concerns.

A common approach to provide security over WiFi link is to bypass WEP (Wired Equivalent Privacy) and use the corporate virtual private networks (VPN). VPNs manage data confidentiality by encrypting network traffic, but they don't always have authentication systems or access controls that work well in wireless environments, especially when the access point may be publicly accessible. [8], [9]. If a VPN is not set up with strong mutual authentication on both ends, subscribers may be open to an attack by a hacker on the WiFi networks, monitoring traffic to the access point, intercepts attempts to connect to the corporate VPN and manages to masquerade as user VPN server, may be long enough to steal logon credentials.

Compared to WEP in IEEE 802.11 WLAN standards, Bluetooth offers a lot more security. Bluetooth devices can transmit private data, for example, schedules between a mobile phone and a PDA. A user does not want anyone to eavesdrop the data transfer. Bluetooth offers mechanisms for authentication and encryption on the MAC layer. The Bluetooth includes a challenge-response routine for authentication, a stream cipher for encryption, and a session key generation. Each connection may require a one-way, two-way, or no authentication using the challenge-response routine, and for each transaction, a new random number is generated on the Bluetooth chip. Key management is not done at MAC layer and it is carried out at higher layers.

The security algorithms use the public identity of a device, a secret private user key, and an internally generated random key as input parameters. To set up trust between the two devices for the first time, a user can enter a secret PIN into both devices. This PIN can have a length of 4 bytes up to 16 bytes. Based on the PIN, the device address, and random numbers, several keys can be computed which can be used as link key for authentication. Link keys are typically stored in a persistent storage. [10]. The authentication is a challenge-response process based on the link key, a random number generated by the device that requests authentication, and the address of the device that is authenticated. An encryption key of a maximum size of 128 bits is generated based on the link key, values generated during the authentication, and a random number. Based on the encryption key, the device address, and the current clock, a payload key consisting of a stream of pseudo-random bits is generated for ciphering user data. The security features included in Bluetooth helps to set up a local domain of trust between devices. If Bluetooth devices are switched on they can be detected unless they operate in the non-discoverable mode. The PINs are quite often fixed. Some of the keys are permanently stored on the devices and the quality of the random number generators has not been specified.

Security in WMANs is a major concern. MAC layer in WMAN includes a privacy sublayer which provides a client/server authentication and key management protocol using digital certificates. Data encryption algorithms includes 3-DES, RSA with 1024-bit key, and AES with 128-bit key. Efficient bandwidth-saving protocols along with use of adaptive modulation in Physical layer, and QoS enable WiMAX reduce jitter and latency, and maintain a consistent bandwidth. Presently AAA needs a ticket based approach. Alternatively service providers may allow ‘first N packets’ before complete verification of a credential that appears legitimate from another trust domain or service provider. Theft-of-service issue demands that AAA needs to be accomplished in parallel with QoS and (security of) Binding Update (for break before make case). Realizing the robust authentication and access control for wireless LANs, the IEEE adapted an authentication system used in wired Ethernet networks. It requires upgraded software drivers in WiFi clients, firmware upgrades or replacement of access points, and the installation of a Radius (Remote Authentication Dial-In User Service) server with public key infrastructure to provide credentials for users.

Using a corporate VPN with 802.1x for authentication and access control is reasonable but not optimal. It can be deployed with only minor changes (the software drivers) to WiFi client hardware, and possibly just firmware upgrades on access points, thus protecting the investment in any WiFi hardware. But for smaller businesses, the need for a Radius server as well as the complexities of VPNs means another solution is needed. New standards may offer just that. The IEEE 802.11i security task group has evolved a standard known as WPA2 for WiFi Protected Access 2 or RSN for Robust Security Network. It would use the Advanced Encryption Standard (AES) for data privacy.

5 Conclusion

Requirements of next-generation (NextG) heterogeneous wireless networks open even more new opportunities for many interesting and comprehensive research topics targeting at concepts, methodologies, and techniques to support advanced mobile value-added services. Clearly, the development of new mechanisms, protocols, algorithms, applications, architectures, and systems will have a significant impact for the successful deployment of emerging wireless networks. Next Generation wireless networks should be able to handle a large volume of multimedia information, having asymmetric data speeds in up and down links, having continuous coverage over a large geographical area, applying quality of service (QoS) mechanism (e.g. efficient encoding, error detection and correction techniques, echo cancellers, voice equalizers), global roaming at low, affordable and reasonable operating costs. Heterogeneous wireless networks should be seamless with regard to transmitting media and open regarding mobile terminal platform and service nodes, and provision of adequate security mechanisms. That would mean that user can freely select protocols, applications and networks. Advanced service providers (ASPs) and content providers can extend their services and contents independent of operators. Location and charging information can be shared among networks and applications.

References:

[1] Suk Yu Hui; Kai Hau Yeung, “Challenges in the migration to 4G mobile systems”, *IEEE Communications Magazine*, Vol. 41, Issue 12, pp 54-59, Dece. 2003.

[2] Varshney, U.; Jain, R., “Issues in emerging 4G wireless networks”, *IEEE Computers Magazine*, Vol. 34, Issue 6, pp94-96, 2001.

[3] L. Gavrilovska, V. Atanasovski, “Interoperability in Future Wireless Communications Systems: A Roadmap to 4G,” *Microwave Review*, 13(1), June 2007, pp.19 – 28.

[4] T. L. Singal, “*Wireless Communications*”, ISBN: 978-0-07-068178-1, Tata-McGraw Hill Education, 2010.

[5] J. M. Pereira, "Fourth Generation: Now, It Is Personal," *Proceedings of the 11th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, London, UK, pp18-21 September 2000.

[6] A. Dutta et al., “Seamless Handover across Heterogeneous Networks – An IEEE 802.21 Centric Approach”, *WPMC 2005*, Aalborg, Denmark, September 2005.

[7] J. Li, H. H. Chen, “Mobility support for IP-based networks”, *IEEE Communication Magazine*, Vol. 43, No.10, Oct. 2005, pp.127-132.

[8] Project: “QoS based Vertical Handoff between WLAN and WiMAX Compatible with the IEEE 802.21 Framework”, Queen Mary, University of London. http://www.elec.qmul.ac.uk/networks/opnet.html

[9] B. G. Evans and K. Baughan, "Visions of 4G”, *Electronics and Communication Engineering Journal*, Vol. 12, No. 6, pp. 293-303, Dec. 2000.

[10] V. Gurbani, X-He Sun, “A system approach for closer integration of cellular and Internet services”, *IEEE Network*, Vol.19, No.1, Jan/Feb. 2005, pp. 26-32.

About the Author

Prof. T. L. Singal is an electronics engineering professional having more than three decades of industrial and teaching experience. An alumni of NIT Kurukshetra, he has many contributions in research & development activities in the field of wireless/telecom technologies with reputed companies in India, Germany and USA during 1981-2002. Since 2003, he is working as Senior Faculty with leading engineering institutes in India. He is the author of two technical books: `**Wireless Communications**' (2010) and `**Analog & Digital Communications**' (2012), both published by International renowned publisher **Tata McGraw-Hill Education**. He has several technical research papers published in International Journals/Conferences including IEEE and convened International/National Conferences in Wireless Networks and Embedded Systems. He is international expert and panel member in various technical journals.