ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Computer Wireless Networking and Communication

Eng.Nassar Enad. GH. Muhanna

Computer Engineer, Computer Department,The Higher Institute of Telecommunication and Navigation, Shuwaikh, Kuwait

Kuwait City, Kuwait

Abstract: This paper presents an overview of wireless networking with emphasis on the most popular standards: Bluetooth, Wi-Fi, WiMAX, and Cellular Networks. A review of what is needed to build a generic wireless network is provided. The literature attempts to discuss the most popular wireless technologies and their protocols. An overview of the advantages that wireless networks have over wired technology is then given. The paper also advances some of the major security risks that wireless networks face. Various strategies that can be employed to mitigate these risks and safeguard the privacy and security of the network are given. A review of how wireless networks can be used in education and training is then given and it is demonstrated that the education field has benefited from the growth of wireless technology and the cost effectiveness of this technology.

I. INTRODUCTION

The invention of the computer and the subsequent creation of communication networks can be hailed at the most significant accomplishment of the 21st century. This invention has transformed the way in which communication and information processing takes place. The network functionality of computer systems has been exploited by the government, businesses, and individual with immense benefits being reaped by all. The two major types of networks in existence are the fixed connection (which makes use of cables) and wireless networks (which use waves to transmit data). The backbone of the vast communication network is made up of fixed connections which mostly utilize fiber optics as well as Ethernet. Even so, wireless networks have gained increased popularity in the course of the past decade. Malone (2004) reveals that as of the year 2000, wireless networks were limited in existence due to the prohibitive cost of wireless devices such as integrated routers and access points and laptops. The hardware cost has significantly decreased making wireless networks affordable to many individuals and organization. In addition to this, technological advances have increased the capacity and efficiency of wireless networks which have made them favorably compare with wired networks. This paper will set out to discuss wireless networking with particular focus on the types of wireless technologies commonly employed and the security measures used to protect wireless technology. A discussion of how wireless technology can be used in education and training settings will also be embarked on.

Computer Networks: An Overview

Computer networks are made up of interconnected computing devices which communicate with each other and these networks are categorized by their sizes. The smallest is the Personal Area Networks (PANs) which extend to a few meters and connect adjacent devices together. Wireless PANs make use of technologies such as Bluetooth to replace cabling as data is moved from device to device. Local Area Networks (LANS) extend from a few hundred meters to a few kilometers and they were designed to cover buildings which are close together or large facilities. Wireless LANs are implemented in facilities such as campuses and busy business locations. Metropolitan Area Networks (MANs) connect different buildings and facilities within a city. These networks mostly make use of wired connections with fiber optic transmissions providing the fastest speeds. The biggest networks are Wide Area Networks (WANs) which connect cities and countries together and they typically make use of fiber-optic cables which operate at speeds of up to 40Gbps.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

What is Wireless Networking?

Wireless networking refers to the "utilization of cross-vendor industry standards, such as IEEE 802.11, where nodes communicate without needing to be wired" (Mamoukaris & Economides 2003, p.1). The infrastructure of wireless networks makes use of standard protocols that are oriented according to the demands of the network. This makes the capacity as well as the quality of services of wireless networks vary based on the devices. Wireless networks are typically expected to deal with devices that are made from various manufactures. The networks are therefore supposed to be able to support different hardware technologies, architectures, and transport protocols and also control the flow of traffic within the network.

All wireless networks make use of waves in the electromagnetic spectrum range. For example, Wireless local-area networks (Wireless LANs) make use of high frequency electromagnetic waves to transmit data. Modulation and demodulation of the radio waves used to transmit data occurs at the transmitter and receiver respectively. They operate in the industry, scientific, and medical (ISM) radio bands and unlicensed-national information infrastructure (U-NII) bands (Zheng 2009). The networks are often connected to routers in order for them to access the internet. Reynolds (2003) declares that Wi-Fi has the potential to let anyone with a computing device to connect to the internet at impressive speeds without the need

Wireless networks also use the Open System Interconnect (OSI) reference model in the transmission of data. The manner in which this reference model applies to wireless networks is similar to wired networks with some differences in the data link layer where wireless networks coordinate access by data to a common air medium and also deal with errors which occur due to the inherent nature of the wireless medium. At the Physical layer, the data is transmitted in the form of radio waves.

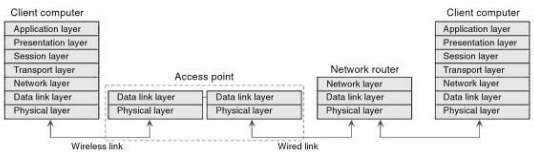

Fig 1: The OSI Protocol Stack and wireless communication

What we need to Build a Wireless Networking

Before a wireless network can be built, it is important to run a site survey. While this step may be ignored when implementing a small wireless network, it is of extreme importance when building a large wireless network. This is because wireless networks operate at the same frequency band used by other equipment such as garage-door openers and microwave ovens and avoiding interference from such equipments is importance if the goal of reliable communication is to be achieved by the wireless network. Ganesh and Pahlavan (2000) note that the largest investment cost in setting up a wireless network is the cost of the physical site location and this deployment is an evolutionary process since the network may need to adjust so as to support an increasing number of users and satisfy the demand for increased capacity and better quality of service. Large networks should be built with manageability and reliability in mind since they may grow to a point where the network administrator is unable to effectively manage them.

There are a number of hardware and software components that are required in implementing a wireless network. One integral hardware device is an access point which is the device linking the wireless network to a wired LAN. Wi-Fi Alliance (2004) notes that the access point is the device that transmits and receives the signals which are used for communicating between the computing devices in the network. Wireless access points have varying capacities and the size chosen is dependent on the speed desired in the network. The device should be placed at a central location and at a high vantage point in order to avoid obstacles and ensure that as many users have access to the network. There are a number of significant factors that one has to consider when acquiring the hardware for the wireless network. Interoperability of the equipment is an important factor if the network is to support all the available protocols (such as 802.11a/b/g). The range which the network is expected to span is also an important consideration. Specifications such as the transmission power and the antenna gain should be used to calculate the range of the equipment.

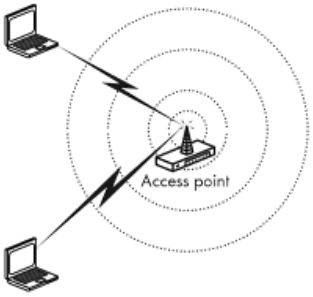

Fig 2: Access Point

In most cases, wireless networks are also connected to the internet. A router which is a device that enables a single internet connection to be shared by many computing devices on the same network is applicable in such a scenario. The range personal networking devices

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

that can access the wireless networks is great and it includes; laptops, personal digital assistants, tablet PCs, and pocket PCs. All the devices accessing the network need to be equipped with an operating system that allows for communication across a wireless network. Wireless access points and the client devices that are connected to them must be properly configured in order for them to operate a TCP/IP network. The wireless clients to a network receive their configuration details from a DHCP which gives the devices their IP addresses, default gateways, and subnet masks. In cases where the administrator wishes to greatly restrict the users, the IP addresses may be imputed manually. Such a move would obviously be very labor intensive and unrealistic for a wireless network that serves a significant number of users.

Wireless Technologies

There are a myriad of wireless technologies and they differ in the amount of bandwidth they provide as well as the distance over which the nodes in the network can communicate. Zheng (2009) observes that wireless technologies also differ in the part of the electromagnetic spectrum that they use and the amount of power consumed. To provide physical connectivity, wireless network devices must operate in the same part of the radio spectrum and two wireless cards therefore need to be configured to use the same protocol on the same channel in order for communication to occur. There are four prominent wireless technologies which are; Bluetooth, Wi-Fi, WiMAX and 3G cellular wireless.

	Bluetooth 802.15.1	Wi-Fi 802.11	WiMAX 802.16	3G Cellular
Typical link length	10 m	100 m	10 km	Tens of km
Typical bandwidth	2.1 Mbps (shared)	54 Mbps (shared)	70 Mbps (shared)	384 + Kbps (per connection)
Typical use	Link a peripheral to a notebook computer	Link a notebook computer to a wired base	Link a building to a wired tower	Link a cell phone to a wired tower
Wired technology analogy	USB	Ethernet	Coaxial cable	DSL

Table 1: Popular Wireless Technologies

- ***Bluetooth***

Bluetooth (IEEE 802.15.1) is the technology that is employed to undertake short-range communication between notebook computers, PDAs, mobile phones and other personal computing devices. The technology is more convenient than connecting devices with a wire to communicate. Bluetooth operates in a license free band at 2.45GHz and the communication range is about 10m and due to this short range, the technology is sometimes categorized as a personal area network (PAN) (Zheng 2009). A major consideration with Bluetooth technology is power usage and typically, the technology provides speeds of up to 2.1Mbps with low power consumption.

- ***Wi-Fi***

Wi-Fi stands for wireless fidelity technology and the term is commonly used to describe a wireless local area network based on the IEEE 802.11 series of standards. The IEEE 802.11 standards resolve compatibility issues between manufacturers of wireless networking equipment by specifying an "over the air" interface consisting of "radio frequency technology to transmit and receive data between a wireless client and a base station as well as among wireless clients communicating directly with each other" (Reynolds 2003, p.3).

Wi-Fi describes a family of radio protocols which include 802.11a, 802.11b, and 802.11g. 802.11b is the most popular wireless networking protocol in use and it uses a modulation called Direct Sequence Spread Spectrum in a portion of the ISM band from 2.412 to 2.484GHz (Zheng 2009). The maximum speed offered by this protocol is 11Mbps with usable throughput of up to 5Mbps. 802.11a is a protocol ratified by the IEEE and it uses a modulation scheme called Orthogonal Frequency Division Multiplexing (OFDM) with a maximum data rate of 54Mbps. It operates in the ISM band between 5.745 and 5.805GHz. The frequency range used by this protocol is relatively unused which makes interference rare. However, Zheng (2009) notes that using this portion of the spectrum is illegal in most countries including the USA. 802.11g is quickly becoming the “de factor standard wireless networking protocol and it is becoming a standard feature for laptops and a lot of hand held devices” (Singh 2009 p.56). The protocol uses the ISM band from 2.412 to 2.484GHz (same as 802.11b) but it uses the OFDM modulation scheme. The maximum data rate for 802.11g is 54Mbps and it is backwards compatible with the popular 802.11b protocol.

- ***Wi-MAX***

A popular form of broadband wireless access for fast local connection to the network is WiMAX. WiMAX is the abbreviation for Worldwide Interoperability for Microwave Access and it was standardized as IEEE 802.16 (Zheng 2009). WiMAX technology has a typical range of 1-6 miles but the technology can span a maximum of 30miles which has made the technology classified as a MAN. This specification has gained great success in the provision of internet access and broadband services through wireless communication systems. WiMAX has a high capacity which makes it efficient in data transmission with speeds of up to 70Mbps being provided to a single subscriber station. The original WiMAX physical layer protocol is designed to propagate

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

signals at a frequency of 10-66 GHz and the technology is able to provide both line of sight coverage and optimal non line of sight coverage as well.

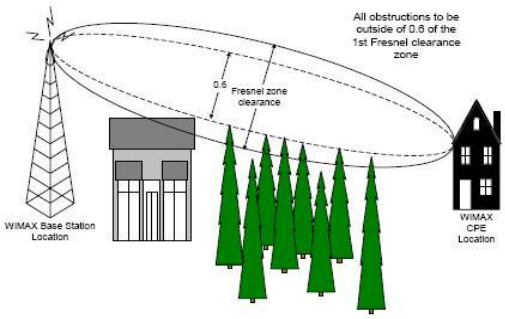

Fig 3: LOS Signal Transmission

The components of a WiMAX include; a Base Station, Subscriber Station, Mobile Subscriber and a Relay Station. The Base station connects and manages access by the devices in the network. This component is made up of multiple antennas pointed in different directions and transceivers which are necessary for the wireless data network communication. A subscriber station is a fixed wireless node which communicates with the base station and forms a link between networks. A mobile subscriber is a wireless node that receives or transmits data through the Base Station while the relay station is a Subscriber Station whose purpose is to retransmit traffic to the relay stations or subscriber stations. A significant merit of WiMAX is that it supports high mobility by user devices. A user can access the network so long as they do not exceed the threshold speed which is normally valued at 120km/H. This property of the technology allows for portability since the user can traverse a significant area which is covered by multiple base stations without having to interrupt their current session.

- ***Cellular Networks***

While mobile phones have gained overwhelming prominence in the past decades, mobile phone networks were introduced as far back as the early 1980s and this technology was able to provide access to the wired phone network to mobile user (Kumar & Manjunath 2008). The area of coverage by the cellular wireless network can range from a few hundred meters to a few kilometers in radius. In each cell, there is a base station which is connected to the wired network and which allows the mobile devices in the range to communicate with each other.

Fig 4: Cellular Transmission Towers.

Until recently, cellular networks were driven primarily by the need to provide voice telephony (Kumar & Manjunath 2008). However, with the growth of demand for mobile internet access, there arose a need to provide packetized data access on these networks as well. While mobile networks were developed with the primary objective of providing wireless access for voice services for mobile users, the growth of the internet as the de facto network for information dissemination has made internet access an integral requirement in most countries. This need has fueled the evolution of mobile networks and the evolution of Mobile Cellular Networks is classified in generations from 1 to 4. The First Generation system was Analog in nature and it was only used for the transmission of speech services. Due to its limitations as well as lack of interoperability between countries, second generation (2G) mobile systems were introduced and these systems supported data transfer capabilities albeit at very low bit rates (Kumar 2010). Owing to the need for increased data rate, the third generation was deployed and these systems had a high data capacity. 3G technology is capable of delivery download speeds of up to 14.4Mbps therefore meeting the demands for high data speeds by consumers. Cellular standards are costly to the user since cellular's use licensed spectrum which are owned by cellular phone operators. Forth Generation mobile system is the latest technology that is still being developed. This technology will have increased capacity and it will try to "integrate all the mobile technologies that exist (e.g. GSM, GPRS, International Mobile Communications, Wi-Fi, and Bluetooth)" so as to harmonize the many services provided and hence enhance user experience (Kumar 2010, p.70).

Advantage of Wireless over Wire Technology

Wireless networks have a number of significant advantages over wired networks. To begin with, it is relatively easier to set up a wireless network infrastructure that it is to make a wired one. This is because the physical devices necessary for wireless networks are less that for wired networks. In installing a wired network, one would need to lay out the cables to connect the devices and this process is not only expensive but also labor and time

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

intensive. Wireless networks require an access point and one the other devices have been properly configured they can operate. Another additional merit of wireless networks is that expansion of an existing network is easy since connectivity is already available within the range of the access point. The ease of deployment of wireless networks makes them economically attractive for most organizations since the capital investment of implementing these networks is not as intimidating that that required for elaborate wired networks. With the wide success of wired LANs, the local computing market has made a steady shift towards wireless LANs which offer the same speeds as wired LANs.

The mobility of wireless networks is another attribute that endears them to users. Wireless networks are built with the consideration that most users who want to access data will be mobile and wired connections may therefore prove to be a major inconvenience. With wireless networks, a person will remain connected as long as they are in within the range of an Access Point. Even so, mobility is not always a requirement for WLANs especially in indoor business settings where the users may be restricted to one physical location all day.

Fifteen years ago, wireless networks were mostly limited to large institutes and government facilities which could afford the prohibitive cost of wireless infrastructure as well as laptops. However, the cost of wireless networks has reduced significantly which has aided in the growth of wireless LANS. It is more economical today to invest in a wireless network infrastructure than it is to set up a wired network which means that more individuals and organizations are opting for wireless networks.

- ***Demerits***

In spite of the advantages that wireless networks possess, there are some major disadvantages which make it necessary to use wired networks in some instances. To begin with, wireless networks are more susceptible to interference when compared to wired networks. Wireless networks make use of radio frequencies and at any given time, there are radio interferences in the atmosphere. The most comply used standard by many WLAN's is the IEEE 802.11b which is an unlicensed radio spectrum that is shared by many consumer devices. These devices which may include cordless phones and baby monitors operate in the same area that most wireless networks are set up. Interferences therefore occur when wireless communication devices have to share frequencies with consumer devices therefore reducing the effectiveness of the network.

II. SECURITY ISSUES

In all forms of communication, security is of vital importance. Securing a network is a challenging task since hardware and software keep evolving and as old threats are overcome, new ones keep presenting themselves. Security implementations of a previous year may therefore not be able to effectively handle the threats being presented in the current years. Wireless networks are prone to a number of security risks and the most significant one is wireless eavesdropping. Due to their wireless nature, it is easier to eavesdrop on them than it is with wired networks. Schmidt and Lian (2009) elaborate that wireless networks are more vulnerable to eavesdropping than wired networks because "access to the network can be gained by proximity rather than a direct physical contact" (p.24). In the case of wired networks, an intruder would have to physically access the network cables so as to eavesdrop. With wireless networks, an intruder simply has to set up his equipment in the area where the wireless signals are being transmitted and from there he can access packets that are intended for other devices in the network. By using a network sniffer, an intruder can capture all network traffic and try to decipher the information contained in the packets. Many wireless networks are insecure with surveys revealing that approximately 60% of wireless networks employed no form of encryption and of the 40% that make use of encryption, 75% of them relied on the WEP which has significant security flaws (Chenoweth, Robert & Sharon 2010).

A good principle is for one to assume that all traffic going through the wireless network is being monitored by unauthorized intruders. With such a consideration, all sensitive information sent through the network should be encrypted. A basic wireless security protocol is the wired Equivalency Privacy (WEP) which essentially provides the same amount of privacy in the wired network as would be obtained in a wired network.

However, WEP can be cracked with relative ease which makes it undesirable for networks where security is of major concern. A solution to this is the Wi-Fi Protected Access (WPA) which is a security framework that presents a more robust protection for the network. The 128bits key length of the WPA is more difficult to break than the 32bit key employed by WEP. The WPA encryption standard gives wireless LAN users' assurance that data transmitted over the network will be encrypted and users authenticated so as to ensure protection from malicious parties. Another significant strength of WPA is that it makes use of Temporal Key Integrity Protocol which means that the unique base keys for each session change periodically in

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

the cause of the session which makes it difficult for an intruder to break into the communication.

The WiMAX technology makes use of an intricate security architecture that is meant to ensure that the network is secure both for Fixed and mobile wireless access. Schmidt and Lian (2009) reveal that the goal of this compact security framework is to create an interoperable security solution that is stable but also accepts the common security protocols. WiMAX security ensures that all WiMAX links are encrypted and a decryption mechanism is required for anyone to read information which is in the network.

In addition to encryption, other strategies can be used to protect wireless network. One approach is the separation of a network and this approach is based on the realization that a wireless network will be open and insecure and it is therefore in the best interest of the entire network that this vulnerable component be isolated. When this approach is implemented, the wired network to which the wireless network is a part of will not be compromised even if the wireless LAN is. Having separate physical infrastructure (hubs, routers, and switches) for the wireless network will ensure that the wireless network cannot be used to compromise the wired network (Jordan & Abdallah 2002). A less expensive means of implementing this is by creating a logical wall of separation between the wireless network and the wired network. In such a set up, the physical devices such as hubs and routers are shared by the wired network's traffic is invisible to the wireless users.

In organizations where security cannot be compromised, extra measures can be applied. Chenoweth et al. (2010) suggests that automated vulnerability assessment applications that verify the security state of the device before users are allowed to authenticate can offer the highest level of wireless security. However, such measures are vey costly to implement which makes many networks avoid employing them.

III. USING WIRELESS TECHNOLOGY IN EDUCATION AND TRAINING

Wireless networks have had a profound impact in the area of schools where the exchange of data was previously unattainable due to the complications associated with wired networked. The education field has benefited from the growth of wireless technology and the cost effectiveness of this technology. Before wireless networks were feasible, the education area suffered from the inherent setbacks of wired networks such as a lack of mobility, the complexity of deployment and difficulty in expanding the network.

There are a number of significant merits of wireless communication in school educational systems. The members of the educational institutes want to access the network for wide ranges of purposes and from various locations. Wireless networks can be less expensive to implement in a school setting that wired networks are. For instance, establishing a wireless LAN in the school may only require the administration to provide the basic connectivity. The users will being their own laptops and therefore save the school money that would have been spent on buying computer hardware as well as Ethernet drops and power outlets. Mamaukaris and Economides (2003) note that with wireless networks, each classroom can be afforded access to the network without need for any major renovations as would be the case if wired networks were to be implemented. All that is required is the placement of access points at strategic points in the classroom buildings. The students will then be able to access the network using their own personal computing devices without incurring additional costs to the schools.

Training sessions may occur in places that are not equipped with wired networks. In such settings, implementing wired networks may be impractical and expensive. Wireless networks can be quickly deployed for temporary use and then moved when the training is over. For small training sessions which have a small number of people, ad-hoc networks can be very useful since they do not require any additional infrastructure to set up. The various individuals in the networks can therefore share resources after configuring their devices to communicate in an ad-hoc manner. This computer networks do not require the use of an access point but rather allow the wireless devices which are within range of each other to discover each other and proceed to communicate in a peer-to-peer manner. Mamoukaris and Economides (2003) argue that implementation so of an ad-hoc wireless networks can help overcome some of the drawbacks caused by the changing educational environment. The networks provide the flexibility and dynamic interaction that is required to foster the success of group communication. However, ad-hoc networks lack a management system which means that the rate of exchange deteriorates as the number of devices in the network increases.

Educational institutes which make use of centralized databases for educational material and information can benefit from wireless networks since the students are able to access the available resources at different areas in the school. Mamaukaris and Economides (2003) demonstrate that the wireless network can be exploited even further by having students connect to the

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

backbone of the school network using their PDAs as they carry out research which will enable them to transfer results of their surveys to a central location in an efficient manner.

CONCLUSION

This paper set out to discus wireless networks which are increasingly becoming preferred over wired networks by many users. The paper began by offering an overview of networking and then proceeded to define wireless networking and discuss the various technologies that are used. From the discussions provided in this paper, it is clear that wireless network solutions are increasing in popularity as they become more affordable and are adopted by more people. This paper has elaborated how wireless networks provide freedom from place restriction, scalability and flexibility. The most popular technologies are; Bluetooth, Wi-Fi, WiMAX and Cellular networks. The paper has confirmed that the mobility of wireless networks is their most desirable characteristic. It has been noted that in spite of their merits, there are a few significant issues with wireless networks which are primarily: quality assurance and security issues. Wireless links are noisier and less reliable than wired links due to the interference that occurs as the signals are transmitted. Engaging in site surveys before setting up a wireless network can help to mitigate this issue. Using strong encryption standards and can resolve the security issues inherent with wireless networks.

REFERENCES

[1]Chenoweth, T Robert, M & Sharon, T 2010, "Wireless Insecurity: Examining User Security Behavior on Public Networks", *Communications of the ACM*, 53(2): 134-138.
[2]Ganesh, R & Pahlavan, K 2000, *Wireless Network Deployments*, Springer, Boston.
[3Jordan, R & Abdallah, C 2002, "Wireless communications and networking: an overview", *IEEE Antenna's and Propagation Magazine*, 44 (1): 185-193.
[4]Kumar, A & Manjunath, K 2008, *Wireless Networking*, Morgan Kaufmann, Boston.
[5]Kumar, A 2010, "Evolution of Mobile Wireless Communication Networks: 1G to 4G", *International Journal of Electronics & Communication Technology*, 1(1): 68-72.
[6]Malone S, 2004, *Case Study: A Path towards a Secure, Multi-role Wireless LAN in a Higher Education Environment*, SANS Institute, Massachusetts.
[7]Mamaukaris, K V and Economides, AA 2003, *Wireless technology in educational systems.* International PEG Conference, St. Petersburg.
[8]Reynolds, J 2003, *Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Network*, CMP, New York.
[9]Schmidt, A & Lian, S 2009, *Security and Privacy in Mobile Information and Communication Systems*, Springer, Boston.
[10]Singh, L 2009, *Network Security and Management*, PHI Learning Pvt. Ltd., New Delhi.
Wi-Fi Alliance, 2004, *WPA Deployment Guidelines for Public Access Wi-Fi Networks*. Wi-Fi alliance, Massachusetts.
[11]Zheng, P 2009, *Wireless Networking Complete*, Morgan Kaufmann, Boston.