Wireless Technology Issues and Concerns: A Business Perspective

Preet Kanwal

Assistant Professor, Department of Computer Science,
Sri Guru Gobind Singh College, Sector-26, Chandigarh-160019, India,
Telephone: 91 172 9814611365; 91 172 2664628,
preetkc@hotmail.com

Abstract

Technology management in an organization involves understanding the value of a certain technology to create a competitive edge for the organization. Faster communication is the key for any business to survive the global competition. With the advancement of computer technology and information exchange worldwide, communication has become possible at a fast pace. The emergence of wireless networks has led to a change in the "backbone" of information services infrastructure being used by individuals and organizations. New wireless communication technologies, inexpensive wireless equipment and wider internet access availability have transformed the way computers and other electronic devices are being used in the organizations, peoples' homes and while on the move. The technology has the potential to provide anywhere, anyplace and anytime information on demand.

Wireless Local Area Networks (WLANs) are being implemented in a wide range of organizations to provide the employees with better and convenient data access while conducting businesses. WLAN can either replace or extend a wired LAN to provide added functionality to a business. The emergence of high rate WLAN communications provide a competitive edge through the wide range of capabilities it provides. This has led to new issues and security concerns, arising from "broadcast" nature of the wireless technology, which augment those of the traditional wired networks.

The wireless communication technologies being used can be categorized on the basis of frequency, bandwidth, range and area of applications. Vendors across the world are providing various products conforming to different WLAN technologies. Before implementing a WLAN in an organization it is necessary to select a suitable technology considering the pros and cons of each. What is to be decided is whether the business needs to upgrade to the wireless technology in an attempt to be more profitable, more operational and more competitive, or if the business can be pushed forward without it. Introduction of any new technology may have some short term limitations caused by its initial integration in the business while re-organizing it. The main concern while shifting to wireless technology is to weigh the short term disadvantages up against the advantages to gauge the long term benefits to be derived from its implementation.

This paper is an endeavor to provide an insight into issues and concerns of integrating wireless technology from organization's perspective. This paper is divided into 5 sections. Section 1 gives an introduction to wireless communication networks and various categories and components of wireless networks. Section 2 provides an introduction to various wireless technologies and standards along with pros and cons of each in brief. Section 3 describes Organizational Application Areas, their Benefits and Concerns. It also details steps for planning the Implementation of Wireless Network in Business Organizations. In Section 4 various Security Risks and Threats involved are discussed. Important steps to be taken towards protection against the risks and threats are also listed. The last section provides the conclusion.

Keywords: Wireless Networking, Wireless Local Area Network, Radio Frequency, Network Interface Card, Bluetooth, Access Point, Hot Spot, IEEE 802.11

1. Introduction

New technologies are being introduced which will affect the way the various businesses operate in the future. Technology management in an organization involves understanding the value of a certain technology to create a competitive edge for the organization. Technology may be in in the form of a new product or service (e.g notebook computers), new business operations (e.g. e-banking) or new production process (e.g online ordering of raw material). "Technology management is the management of innovation, whether it is a product, a process or an organization, from its conception to its diffusion, and therefore to its implementation within the company, including the consequemnces , advantages and disadvantages for all variables and actors involved in running the company."[1] Organizations choose to adopt new technologies for adding value to procedures and services offered. The factors leading to technology shift are: Increased productivity, reduced workforce, reduced waste, higher income and profits, advanced communications and finally a competitve edge. The factors which might restrain an organization are: integration, management and maintenance of technology, skill updation, costs and time involved in impelemntation. One of the major impact on the business and industrial organizations has been caused by the convergence of information technology and media or broadcasting. Wireless is offering new cost advantages, availability of information on demand as per need, flexibility in responding to changes in IT infrastructure needs. The emergence of wireless networks has led to a change in the "backbone" of information services infrastructure being used by individuals and organizations.

Wireless Local Area Network (WLAN) is a flexible data communication system that can either replace or extend a wired LAN to provide added functionality. WLANs transmit and receive data over the air, through wall, ceilings, and even cement structures using Radio frequency (RF) technology, or Infrared (IR) instead of wired cabling. A WLAN provides all the features and benefits of traditional LAN technologies like Ethernet and Token Ring, but without the limitations of being connected by a cable. This provides greatly increased freedom and flexibility.

Wireless networks are becoming more pervasive, accelerated by new wireless communications technologies, inexpensive wireless equipment and broader internet access availability. Wireless is offering new cost advantages, availability of information on demand and

when needed, flexibility in responding to changes in IT infrastructure needs. It is on way to becoming the backbone of information services infrastructure. These networks are transforming the way people use computers and other personal electronics devices at work, home and while traveling.

1.1 Categories of Wireless Networks

There are many wireless communications technologies that can be differentiated by frequency, bandwidth, range and applications. There are four main categories of connectivity provided by wireless networks based on the range of distance they cover as described in the Table below:

Table 1: Categories of Wireless Networks[2]

Category	Name	Range	Application
WPAN	Wireless Personal Area Network	1 m	Connecting and Controlling various products and devices via Bluetooth and Infrared
WLAN	Wireless Local Area Network WiFi Networks (IEEE 802.11)	100 m	LAN on a floor of the building
WMAN	Wireless Metropolitan Area Network (IEEE 802.16)	1 Km	Suburbs of a city connected to internet via broadband
WWAN	Wireless Wide Area Network	10 Km	GSM Mobile Phone, CDMA

1.2 Components of a Wireless Network System

A wireless network consists of several components[3] that support communications using radio or light waves propagating through an air medium with the exception of the wire from the ISP to the broadband modem and from there to the router. Some of the elements overlap with those of wired networks. Wireless Networks Include Users, Computer Devices, Base Stations, and a Wireless Infrastructure.

- **User** - A user can be anything that directly utilizes the wireless network.
- **Computer Devices** - mobile devices, desktops, servers, databases, and websites.
- **Network Interface Card (NIC) -** provides the interface between the computer device and the wireless network infrastructure.
- **Air Medium** - Wireless information signals travel through the air, the quality of transmission, however, depends on obstructions in the air that either lessen or scatter the strength and range of the signals.
- **Infrastructure -** The infrastructure of a wireless network interconnects wireless users and end systems. The infrastructure consists of base stations, access controllers, application connectivity software, and a distribution system.
- **Base Station -** interfaces the wireless communications signals traveling through the air medium to a wired network—often referred to as **a distribution system**. . An **access point** or a **hot spot** provides an interface with systems within the infrastructure and users associated with other access points.
- **Access Controller -** is hardware that resides on the wired portion of the network between the access points and the protected side of the network. It regulates traffic between the open wireless network and important resources.

- **Application Connectivity Software -** is necessary as an interface between a user's computer device and the end system hosting the application's software or database.
- **Distribution System –** connects wireless and wired parts to tie together the access points, access controllers, and servers.

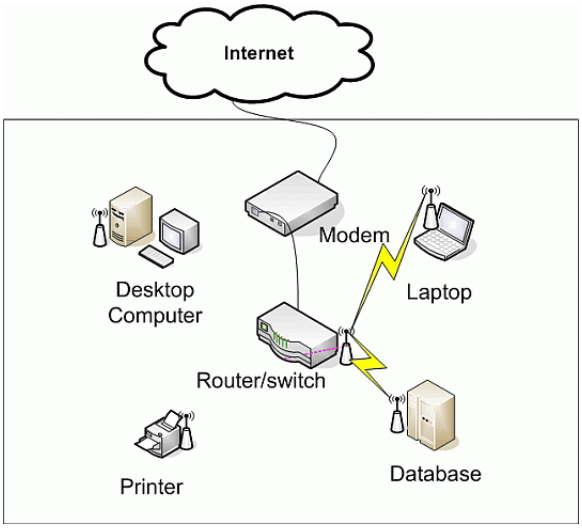

Figure 1 – A Wireless Network
(Source: Computer Help and Technical Support for Everyone, retrieved from www.ask-the-computer-doc.com/lan-definition.html)

2. Technologies and Standards

Over the years, WLAN infrastructures are being implemented into offices and homes to provide more convenience and better communication of data across their LAN. Various Technologies and Standards to be used for communication on the wireless network have evolved.

2.1 Wireless Technologies

The process by which radio waves are propagated through the air, the amount of data carried, immunity to interference from internal and external sources, and a host of other characteristics varies from technology to technology. Wireless technologies[4] can be differentiated according to:

- **Protocol** – Asynchronous Transfer Mode (ATM) or Internet Protocol (IP)
- **Connection type -** Point-to-Point (P2P) or multipoint (P2MP) connections
- **Spectrum** - Licensed or unlicensed

Spread spectrum is a method used to modulate or splitting the information into manageable bits that are sent wirelessly over a series of radio channels or frequencies. The information is demodulated, or combined at the receiving end of the radio system. Two kinds of spread spectrum are available:

- **Direct Sequence Spread Spectrum (DSSS)** -This method divides the 2.4GHz band into 14 twenty-two MHz subchannels with no hopping between subchannels. Data is sent

through one 22MHz channel. Channels are centered at 5 MHz spacing, giving significant overlap. The advantage of this technique is that it reduces the effect of narrow band sources of interference.

- **Frequency Hopping Spread Spectrum (FHSS) -** The FHSS method works by dividing the 2.4GHz bandwidth into 75 subchannels of 1MHz bandwidth each. Each sender/receiver pair in the network medium selects a different frequency-hopping pattern, minimizing the chance of two pairs using the same subchannel.

Frequency-Division Multiplexing (FDM) system, the available bandwidth is divided into multiple data carriers. The data to be transmitted is then divided among these subcarriers. A frequency guard band is placed around each carrier which lowers the bandwidth efficiency. In some FDM systems, up to 50 percent of the available bandwidth is wasted. In most FDM systems, individual users are segmented to a particular subcarrier; therefore, their burst rate cannot exceed the capacity of that subcarrier. If some subcarriers are idle, their bandwidth cannot be shared with other subcarriers.

Orthogonal Frequency Division Multiplexing (OFDM) - delivers up to 54 Mbps data rates in the 5MHz band. OFDM is a coding or transport scheme which divides a single digital signal across 1000 or more signal carriers simultaneously. The signals are sent at right angles to each other so they do not interfere with each other. The benefits of OFDM are high spectral efficiency, resiliency to RF interference, and lower multipath distortion.

2.2 Wireless Standards for Business Organizations

The Institute of Electrical and Electronics Engineers (IEEE) Standards Association is a major developer of a broad range of industrial standards. A set of wireless standards[5] under group name **IEEE 802.11** – for wireless LAN's - is the most prevalent standard for providing wireless solutions for business organizations and uses 2.4 GHz radio signaling frequency. Other commonly used standards are RFID and Bluetooth. A brief about these standards is given below:

IEEE 802.11a

- For Business Market and has Higher Cost
- Operates in the higher 5GHz unlicensed radio band.
- Fastest Maximum speed and More Simultaneous Users support
- Regulated Frequencies stops interference from other devices
- Range signal is short and Signal can easily be blocked

IEEE 802.11g

- Similar to 802.11a, Operates in lower 2.4GHz unlicensed radio band
- Uses Orthogonal Frequency Division Multiplexing (OFDM) – which breaks a wide frequency channel into several sub channels and transmit data in parallel
- Backward compatible with 802.11b
- Extends the maximum data rate (signaling speed) from 9 Mbps to 54 Mbps making it possible to serve upto five times as many users
- Its throughput falls off slowly with distance as compared to 802.11a

IEEE 802.11n

- Based on Multiple input / Multiple Output (MIMO) OFDM technology
- Transmission rate of the order of 100 Mbps upto 600 Mbps

- Increased range of operation

RFID - Radio Frequency Identification

- Chips are read by radio over short distances
- Provide real-time data for many information systems
- Radio signals may experience problem passing through solid walls
- Excessive implementation cost

Bluetooth

- Designed to serve personal area networks upto 10m
- Poor Scalability - serves only few devices carried by a person
- Lower cost and lower battery drain
- Interferes with 802.11b networks as it uses the same 2.4 GHz unlicensed radio band

3. Organizational Application Areas and Implementation

The core of organizations in developing and launching wireless systems is to deal with large amount of information and to make that information easily accessible to users. Subsequently, wireless network seems to be a probable solution as it generates added channels for the smooth flow of information. The wireless networks can be used by business and other organizations as framework to support other developing technologies like the use of RFID tags, VoIP (Voice over IP) networks

The challenge faced by the business organizations is to install wireless networks that are uncomplicated to use, safe, abide by the existing business standards, are flexible enough to become accustomed to a extremely sundry patrons, and which do not put too much of a service and support burden on the existing workforce.

3.1 Application Areas and related Business Benefits

The organizations can use wireless mobility as a way to gain business advantage to enhance productivity, collaboration, and responsiveness to market changes and competition through real time data access.

Wireless networking is especially useful in areas where there are constraints for laying cables like in manufacturing units, hospitals. It is also useful for those organizations which have to relocate to new locations and premises in accordance with the changing needs of their business. It can also help staff in office environments. A wide range of industrial and other organizations can benefit by integrating wireless technology in their business and office procedures. Some of the major application areas are:

- **Financial Sector Organization –** Wireless access can enable the Financial-services organizations to provide their employees an instant access to industry trends, customer data, and financial information. This would help the business organization to dramatically improve customer service and quicker delivery of their products and services.
- **Government Sector**– With rapid development in the telecommunication and business environment, the global environment has changed. The role of the Government in facilitating and guiding the competition as well as protecting the consumer has evolved to a new dimension. Wireless technology can provide Public-safety and law-enforcement

agencies with uninterrupted secure access to crucial information which further helps them in reducing response time to efficiently respond to a crisis situation or day-to-day operations.

- **Manufacturing and Retail Industries -** Wireless networked supply chains helps the manufacturers in enabling their employees to share real-time data on the factory floor and support timely assembly. Wireless networks also allow retailers to improve flexibility and efficiency of their stores' procedures. It allows faster check on customers as well as providing the customers with access to relevant product information, and a faster online ordering system.
- **Healthcare –** Healthcare is one area which can immensely benefit from use of wireless technology. Wireless LANs can help in tracking valuable medical equipment for timely availability. The healthcare providers can access real-time patient information as well as status of medical research to improve in reaching accurate decisions and to provide timely quality healthcare.
- **Transportation Industry –** The various components involved with transportation viz. Airlines, railroads, commercial trucking firms, and other businesses have integrated wireless networks to make their workforces more efficient by being mobile. Wireless LANs improve efficiency of cargo handling, warehousing, and shipping through automation which in turn improves customer service.
- **Education -** Wireless networks in educational institutes provide a wide range of applications throughout their facilities without expensive rewiring. It enables the students and staff access to enhance learning, research and administration through e-learning, voice communications and high-bandwidth Internet access. Educational institutes can secure their libraries as well as make it user friendly by means of RFID wireless technology.
- **Office Environment** – The users and staff who are always on the move to different locations can access the network and connect to their base office without going through the hassle of plugging into wired network while moving through transportation systems, cafés, restaurants, or hotels.
- **Overall Organizational Benefits -** Wireless solutions have the potential to help increase revenue and control costs to increase productive time inside the organization. Wireless networks facilitate real-time access to people, applications, and network resources across campuses, branch offices, and remote locations using a variety of devices. It provides faster access of information to users through enhanced database and multimedia resources access. One of the main overall benefits is that the wireless network is more easily upward scalable to support upto the maximum number of computers stated on the hub or router than a wired network.

3.2 Areas of Concerns

There are certain concerns to be taken into account while installing wireless networking in Business Organizations:

- Safety, Security and Authenticated user access
- Centralized management and monitoring of resources
- Bandwidth Management for faster resource sharing
- Cost of implementation, service and subsequent support
- Compliance and Conformity with the standards

3.3 Planning and Implementing a Wireless Network in a Business Organization

The first and foremost step to deploy a wireless network in any organization is to do a feasibility study in terms of business resources, users' demands, costs involved and benefits over and above the existing system. Thereafter the following steps should be undertaken in planning and implementation of a wireless network.

i. Understand the needs of the consumer as well as the business processes in the current business environment.
ii. Constitute a WLAN team comprising of departmental personnel, IT personnel, and a Network administrator. The network administrator should be familiar with the business processes, networking technologies and standards to provide the best solution in accordance with the particular business organization.
iii. Consult a wireless communication professional and solution provider to ensure compliance with the safety and security norms. Develop a clear and well-organized wireless policy.
iv. As the wireless network communicates via radio frequency using air as medium, conduct site survey of the business locations taking into consideration obstructive structures, such as large buildings, water, office furniture, thick walls, heavy machinery, store materials, hospital sensitive equipment, natural elements like trees etc. in order to identify poor signal, signal interference and no signal areas. Specify the locations where high bandwidth is required.
v. Evaluate the number of connected devices, range of the application and number of users. Select the system components that are compatible with existing hardware and software of the business organization. Be sure the selected systems meet the future demands of wireless network.
vi. Conduct periodic training programs to educate staff and users on using the wireless networks.

4. Security Risks and Threats

Although wireless-enabled devices enhance productive value outside office or home, yet it can also expose the user to a number of security threats as a result of using a public access point. The 802.11b standard offers low cost, strong performance and ease of deployment and thus is widely prevalent as preferred technology standard. It shares unlicensed frequencies with other devices including Bluetooth, cordless phones leading to interference amongst these technologies. All this makes it easier for attackers to mount an attack on wireless network.

4.1 Wireless Network Threats[6]

- **Insertion attack** - Failure to secure wireless network potentially opens the internet connection to a surprising number of users with a wireless-enabled computer within range of the wireless access point being used to hop a free ride on the internet over the user's wireless connection leading to service violations by exceeding the number of connections permitted by the internet service provider, Bandwidth shortage and slower connection. Malicious user may monitor the internet activity to steal sensitive information, install spyware or take control of the organization's computer and engage in illegal activity that will be traced to the owner of the connection.

- **Broadcast Monitoring -** a specific kind of insertion attack where malicious users' drive through cities and neighborhoods with a wireless-equipped computer searching for unsecured wireless networks and publish the location information on web sites to perpetrate illegal online activity using other's connection to mask their identities.
- **Jamming -** A wireless network may be subjected to jamming in situations where legitimate traffic gets jammed as a result of overwhelming flow of illegitimate traffic thus resulting in a kind of denial of service to legitimate users.
- **Access Point Clone or Evil Twin Attacks - T**he attacker gathers information about a public access point, then sets up his or her own system by broadcasting signal stronger than the one generated by the real access point. Unsuspecting users will connect to the network using the stronger, bogus signal through the attacker's system that may use specialized tools to read any data the victim sends over the internet.
- **Sniffing -** Many public access points are not secured properly and the traffic they carry is not encrypted thus putting sensitive communications or transactions at risk and open to malicious users to use "sniffing" tools to obtain sensitive information such as passwords, bank account numbers, and credit card numbers.
- **Client-to Client Adhoc Connections -** Many laptop computers, particularly those equipped with 802.11-type WiFi wireless networking cards, can create ad hoc networks of client-to-client when within each others range. Manufacturers set the wireless cards to ad hoc mode by default. An attacker with a network card configured for ad hoc mode and using the same settings as authentic user's computer may gain unauthorized access to his sensitive files.
- **Unauthorized Computer Access-** An unsecured wireless network combined with unsecured file sharing can spell disaster where a malicious user could access any directories and files allowed for sharing by the user.
- **Shoulder Surfing -** In public wireless areas, conducting personal business in a public space provides opportunity for malicious users to glance over user's shoulder or, peer through binoculars from some distance to steal all kinds of sensitive, personal information.

4.2 Protecting Wireless Networking

The following are some steps to safeguard against security threats of connecting to a wireless network's public access point or Hot Spot:

- Make sure the organization's router's security settings are enabled.
- Ensure that appropriate firewall, Virus and Anti-Spyware softwares have been installed and set up.
- Change the default system ID (SSIS - service set identifier or ESSID - extended service set identifier) of the wireless access point or router.
- Change the default password for your system.
- Turn off identifier broadcasting of the Wireless access point.
- Encrypt wireless communications. Use the router's built-in firewall to restrict access to your network.
- Keep the wireless system patched and up to date.
- Use File sharing with caution, encrypt files and disable file sharing when connecting to a public wireless access point.

- Use a virtual private network (VPN) if possible- VPNs encrypt connections at the sending and receiving ends, and keep out traffic that is not properly encrypted.
- Avoid using passwords and providing personal information to web sites.
- Be aware of the immediate surroundings.

5. Conclusion

Wireless Local Area Networks are being implemented in the organizations and homes to provide better and convenient data access. The emergence of high rate WLAN communications provides a competitive edge through its wide range of capabilities. This has led to new issues and security concerns arising from the "broadcast" nature of the wireless technology to augment those of the traditional wired networks. Establishing organizational support for deployment of wireless networking in a business is critical. The shift should be done in phased manner in order to give staff and users the necessary time to adjust to the new policies, standards and limitations on choices for devices, data carriers, and available service plans. In future, enhanced WLAN management technology would enable users to have better mobility and security alongwith more well-organized transmission of data.

Notes and References

1. Chanaron, J.J. and Grange, T., "Towards Redefinition of Technology Management", Author manuscript, published in The 3rd IEEE International Conference on Management Innovation and Technology, Singapore: Indonesia 2006.
2. Quinn, L., Mehta, P., and Sicher, A. "Wireless Communications Technology Landscape" Dell White Paper February 2005, pp 1.
3. Geier, J.,"Wireless System Architecture: How Wireless Works" , Sample Chapter provided courtesy of Cisco Press., pp. 1., accessed on http://www.ciscopress.com/articles
4. CISCO - Internetworking Technologies Handbook, Chapter 20 pp 20-1
5. Choi, Y.B., Park, J., Fernandez, D. and Kim, K., "Recent Wireless LAN Management Technologies: Trends and Outstanding Issues", Issues in Information Systems, Volume VI, No. 2, 2005 pp 331-334
6. **"**Using Wireless Technology Securely**",** Produced 2006 by US-CERT, a Government organization.Updated 2008. pp 1-2