*Available online at www.journalijmrr.com*

**INTERNATIONAL JOURNAL OF MODERN RESEARCH AND REVIEWS**

***Int. J. Modn. Res. Revs.***

***Volume 5, Issue 6, pp 1580-1582, June, 2017***

**ISSN: 2347-8314**

**ORIGINAL ARTICLE**

# WIRELESS NETWORKS LAN IMPLEMENTATION AND SECURITY MEASURES

***P.Balamurugan and Desta Dana**

School of Informatics, Wollaita Soda University, Ethiopia

***Article History:*** *Received 7th June ,2017, Accepted 29th June,2017, Published 30th June2017*

**ABSTRACT**

Wireless networks may seems to be a simpler alternative to networking a school than a cabled network, however schools should not install wireless networks unless they are aware of the potential issues and satisfied that it is the right decision for the school. Wireless networks are significantly slower than fixed networking, by a factor of approx 10. Wireless is also less reliable than cabled networks mainly due to issues such as the movement of mobile PCs and possible reductions in signal strength due to changes in the local environment. Wireless networks are typically not suitable for schools with thick walls, including many older schools. As wireless data travels through the air, there is a risk it could be accessed by other parties at ranges of 100-300 metres outside of the school grounds. There is thus a risk that sensitive school or pupil data could be accessed by unauthorised parties. In order to prevent such an occurrence high quality wireless security software would need to be installed by qualified companies who can provide the appropriate level of technical support and maintenance to schools. Too often schools install wireless networks with either no or inadequate levels of security. The most obvious difference between wireless and wired networks, therefore, is that the latter uses some form of cable to connect computers together. A wireless network does not need cable to form a physical connection between computers. Wireless networks can be configured to provide the same network functionality as wired networks, ranging from simple peer-to-peer configurations to large-scale infrastructures accommodating hundreds of users.

**Keywords:** Wireless networks, LAN, wireless security

## 1.INTRODUCTION

When the term *'wireless network'* is used today, it usually refers to a wireless local area network (WLAN). A WLAN connects computers together through radio technology using standard network rules or protocols, but *without* the use of cabling to connect the computer together.

Wireless technology has helped to simplify networking by enabling multiple computer users to simultaneously share resources in a home or business without additional or intrusive wiring. These resources might include a broadband Internet connection, network printers, data files, and even streaming audio and video. This kind of resource sharing has become more prevalent as computer users have changed their habits from using single, stand-alone computers to working on networks with multiple computers, each with potentially different operating systems and varying peripheral hardware. U.S. Robotics wireless networking products offer a variety of solutions to seamlessly integrate computers, peripherals, and data. Laptop users have the freedom to roam anywhere in the office building or home without having to hunt down a connector cable or available jack. Every room in a wireless home or office can be "connected" to the network, so adding more users and growing a network can be as simple as installing a new wireless network adapter.

**Reasons to choose wireless networking over traditional wired networks include:**

- Running additional wires or drilling new holes in a home or office could be prohibited (because of rental regulations), impractical (infrastructure limitations), or too expensive.
- Flexibility of location and data ports is requiredRoaming capability is desired; e.g., maintaining connectivity from almost anywhere inside a home or business.
- Network access is desired outdoors; e.g., outside a home or office building

**Wireless LANs in the Office**

An 802.11 network is the ideal solution for a network administrator in many respects. No longer is it a requirement that every workstation and conference room be wired up to

**Corresponding author:Mr.* ***P.Balamurugan,*** *Associate Professor, School of Informatics, Wollaita Soda University, Ethiopia*

hubs and switches with cables in hard-to-reach areas. Wireless networking allows for impromptu meetings in cafeterias, hallways, courtyards, or wherever inspiration strikes while providing real-time LAN connectivity for business applications such as sending e-mail, working on spreadsheets on shared drives, and conducting market research.

**Wireless LANs in the Home**

Wireless networking has become commonplace, and with prices reduced to a fraction of what they were, it is no wonder that wireless networking products have transitioned from the office and into the home. For the home user, a wireless network provides freedom in convenience and lifestyle to exchange words, data, and music or video with any computer – across the Internet, or around the world. Home users can create a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout the home on multiple computers, making it more convenient for everyone to get online.

## 2.RESULT AND DISCUSSION

**Wireless LAN Frequency Usage**

The 802.11b standard defines 14 frequency the FCC (Federal Communications Commission) and IC (Industry Canada) allow manufacturers and users to use channels 1 through 11, per ETSI approval (European Telecommunications Standards Institute); most of Europe can use channels 1 through 13, while in Japan, users have all 14 channels available channels for use with this technology. Depending on the country a user lives in and where he or she will be installing a WLAN, there are certain governmental restrictions for companies offering these products and consumers or businesses deploying these products. As a result, the bandwidth required for each channel signal overlaps several adjacent frequencies. This leaves the typical U.S. user with three channels available for use by access points (channels 1, 6, and 11) that are within radio range of adjacent access points.

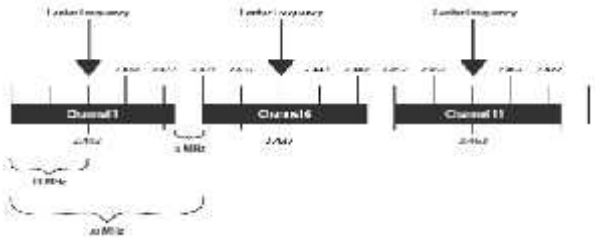

**Fig: Bandwidth required for each 802.11 channel (also demonstrates the 5 MHz between each frequency)**

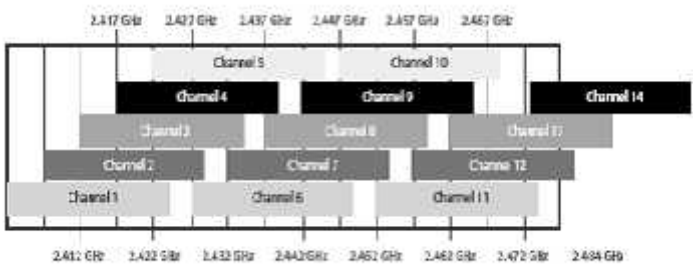


**Fig: Shows an example of overlapping frequencies —802.11b bandwidth allocation**

**Ad Hoc (Peer-to-Peer) Mode vs. Infrastructure Mode**

The 802.11 specification defines two types of operational modes: ad hoc (peer-to-peer) mode and infrastructure mode. In ad hoc mode, the wireless network is relatively simple and consists of 802.11 network interface cards (NICs). The networked computers communicate directly with one another without the use of an access point. In infrastructure mode, the wireless network is composed of a wireless access point(s) and 802.11 network interface cards (NICs). The access point acts as a base station in an 802.11 network and all communications from all of the wireless clients go through the access point.

**Infrastructure Mode**

In infrastructure mode, all mobile and wireless client devices and computers communicate with the access point, which provides the connection from the wireless radio frequency world to the hard-wired LAN world. The access point performs the conversion of 802.11 packets to 802.3 Ethernet LAN packets. Data packets traveling from the LAN to a wireless client are converted by the access point into radio signals and transmitted out into the environment. All wireless clients and devices within range can receive the packets, but only those clients with the appropriate destination address will receive and process the packets. A basic wireless infrastructure with a single access point is called a Basic Service Set (BSS). When more than one access point is connected to a network to form a single sub-network, it is called an Extended Service Set (ESS).

**Wireless Network Components**

There are certain parallels between the equipment used to build a WLAN and that used in a traditional wired LAN. Both networks require a network interface card (NIC) that is either built-in to or added to a handheld, laptop or desktop computer. There are two main types of plug-in card available: PCMCIA which is inserted into the relevant slot in the side of a laptop and

PCI which is inserted into one of the internal slots in a desktop computer. Wireless NICs contain an in-built antenna to connect with the network. In a wireless network, an *'access point'* (AP) has a similar function to the switch in wired networks. It broadcasts and receives signals to and from the surrounding computers via their wireless NICs. It is also the point where a wireless network can be connected into an existing wired network.

**Access Point**

The access point is a device that links a wireless network to a wired LAN. It increases the effective range of a wireless network and provides additional network management and security features. Wireless networks of three or fewer PCs do not require an access point for ad hoc networking.

**PC Card**

A wireless PC card enables laptop users to connect wirelessly to the LAN. U.S. Robotics

22 Mbps Wireless PC Cards allow for adhoc networking of up to three computers at an effective range of up to 1000 feet in open spaces.

**PCI Adapter**

Just as a wireless access PC card allows portable and laptop computers access to the LAN, a wireless access PCI adapter allows desktop PC users access to the LAN. U.S. Robotics 22 Mbps Wireless PCI Adapters allow for ad hoc networking of up to three computers at an effective range of up to 1000 feet in open spaces.

**Wireless Security**

Security is an obvious concern with any network, wired or wireless. Because communication over a traditionally wired network is, by its very nature, over physical wires, security is often built into the physical environment itself. WLANs operate over radio signals, so the same security measures cannot be assumed. For many wireless users, the enabling of the built-in security known as Wireless Equivalent Privacy (WEP) is sufficient for their home or small to medium office WLAN. WEP uses 64- and 128-bit encryption and is the cipher scheme designated for use in 802.11b networking. U.S. Robotics 22 Mbps wireless products include enhanced 256-bit WEP encryption that is not commonly. Move Access Point in Front of Firewalls or DMZs: The best solution for keeping prying eyes away from a corporate network is to move the access point off of the corporate LAN and in front of a firewall or on a DMZ (demilitarized zone) port. With the access point in front of a firewall, intruders will not have access to the corporate LAN. All corporate wireless users will require the installation and use of a virtual private network (VPN) client to create a secure tunnel into the corporate LAN. This may require additional administrative support from IT personnel, but the extra security is well worth the effort.

**Security concerns**

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received --much less decoded-- by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all.

However, eavesdropping is possible using specialist equipment. To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption that provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels. Several industry players have recently offered secure wireless solutions.

**Advantages of wireless LANs**

- Very flexible within the reception area
- Ad-hoc networks without previous planning
- possible
- (almost) no wiring difficulties (e.g. historic
- buildings, firewalls)
- More robust against disasters like, e.g.,
- Earthquakes, fire - or users pulling a plug...

# 3.CONCLUSION

The level of flexibility will of course depend on the variety of wireless access point locations but wireless LAN users recognize the increased convenience and the boost to productivity allowed by their ability to access the network from a multitude of locations. The improvements in the quality of work that wireless LAN users underline results primarily from improved accuracy. By using a wireless LAN, data can now be fed directly from various locations instead of being manually input at a later date.

**Information source**


1. *For additional information on IEEE wireless activity, standards, and development, visit the IEEE Web site at: http:// standards.ieee.org/ wireless*
2. http://www.vicomsoft.com/knowledge/reference/wireless1.html*track=internal
3. http://www.webopedia.com
4. Bob Liu, 802.11g-reenlighted After Task Group Battle, www.80211-planet.com
5. Wireless LANs: Improving Productivity and Quality of Life, www.wlana.com