DESIDOC Journal of Library & Information Technology, Vol. 31, No. 1, January 2011, pp. 41-48

REVIEW PAPER

Current Trends in Wireless Technologies in Academic Libraries

M. Krishnamurthy and H.M. Rajashekara*

Documentation Research and Training Centre
Indian Statistical Institute, Bengaluru-560 059
E-Mail: mkrishna_murthy@hotmail.com

**Central Computer Centre*
Indian Statistical Institute, Bengaluru-560 059
E-Mail: raja@isibang.ac.in

ABSTRACT

Wireless communication is the transfer of information over a distance without the use of wires. Wireless communication is generally considered to be a branch of telecommunications. Wireless operations permit services, such as long-range communications that are impossible or impractical to implement using wires. Wireless communication brings fundamental changes to data networking and telecommunications, and makes integrated networks a reality. Wireless networks focus on networking and user aspects. Network architecture for personal communication systems, wireless LANs, radio, tactical and other wireless networks, and design and analysis of protocols are addressed on a regular basis. At present, the major application of Wi-Fi implementation in libraries is limited to information management. This paper elaborates the Wi-Fi in detail about the components, functions, area of applications, issues, and challenges.

Keywords: Wi-Fi technology, ICT, WiMAX, local area network, standards , access point

1. INTRODUCTION

Features of the emerging knowledge society of the digital era include the convergence of information and communication technologies (ICTs) enabling almost seamless access, in the expanding digital space, to vast and varied information and knowledge sources from anywhere, at any time. The spread of telecom facilities—wireless technology and cellphone—into rural areas is enabling rural traders and others to obtain market information for their products, to contact village and/or taluq and district officials, not only to get information but also to obtain certificates and other documents[1]. Availability of ICTs in developing countries is not as widespread as it is in Europe and North America. However, the spread of wireless technologies, especially cell phones, has been rapid. New areas and new groups of users are able to access ICT services including wireless local area networks, and long-range wireless links in libraries and information centres.

The idea of increasing the effectiveness of information exchange by sharing the work nationally and internationally is fully recognised, but the planning of information activities on such a scale must take into account the perspective of national and international cooperation. There has been a growing concern for improvement of library services in general and scientific and technological library services in particular for providing effective and efficient information support for carrying out research and education activities. In addition, such information system requires both the use of modern scientific information theory and advanced technology[2].

2. WHAT IS WI-FI TECHNOLOGY?

Wireless technology is an alternative to wired technology, which is commonly used, for connecting devices in wireless mode. Wi-Fi (Wireless Fidelity) is a generic term that refers to the IEEE 802.11 communications standard for Wireless Local Area Networks (WLANs).

Wi-Fi is wireless technology gives connections to the Internet and Intranet using low power radio waves. Wi-Fi network connects computers to each other, to the

Received on: 25 August 2010

Internet, and to the wired network. LANs have been available since the late 1980s, but the market remained immature due to dearth of standards and predominance of incompatible proprietary solutions. By definition, LANs are local in terms of networking technology and thus involve none of the complexities of routing, Internet work address resolution, name-to-address translation, segmentation, reassembly of data packets, etc. Also, since traditional LANs have been bound by the limitations of physical media, such as the 500 meter maximum coaxial cable length for a traditional 10-BASE 5 Ethernet, user mobility has not traditionally been an important consideration.

3. CLASSIFICATION

There are a lot of entities describing wireless communication for WLANs. Among the famous standards that the IEEE certifies are standards 802.11a, 802.11b and 802.11g. WLANs, based on the Wi-Fi technologies are often implemented as an overlay to the wired LAN based on the Ethernet technology. There are two main architectures used in the WLAN environment:

(a) Peer-to-peer autonomous architecture in which the wireless access point (AP) has autonomy over access, security, and operation. APs in this architecture usually do not require a wireless controller.

(b) Centralised WLAN architecture in which lightweight APs with limited functionality are used, with most of the wireless intelligence residing at a central controlling device, i.e., the WLAN controller.

Any wireless network can be thought of as a combination of one or more of the following types of connections:

(i) Point-to-point: The simplest connection is the point-to-point link. These links can be used to extend a network over great distances.

(ii) Point-to-multipoint: When more than one computer communicates with a central point, this is a point-to-multipoint network.

(iii) Multipoint-to-multipoint: When any node of a network may communicate with any other, this is a multipoint-to-multipoint network, (also known as an ad hoc or mesh network) which allows for much greater bandwidth.

Wireless networking (i.e., the various types of unlicensed 2.4 GHz, Wi-Fi devices) is used to meet a variety of needs. The most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling.
- To provide a backup communications link in case of normal network failure.
- To link portable or temporary workstations.
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

The Wireless communication can be via:

- Radio frequency (RF) communication.
- Microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication, or
- Infrared (IR) short-range communication, for example from remote controls or via Infrared Data Association (IRDA).

Application may involve point-to-point communication, point-to-multipoint communication, broadcasting, cellular networks, and other wireless networks.

4. CHARACTERISTICS

4.1 Wi-Fi Hotspot

The term 'hotspot' refers to the referral to the area or physical location where an access point is made accessible to users with Wi-Fi enabled devices, typically found in coffee houses, airports, hotels, malls, and increasingly in libraries. Wi-Fi hotspots are places where users can visit anytime for fast and reliable broadband wireless Internet access. Wi-Fi hotspot services are available in places such as Internet cafes, coffee houses/shops, and airports around the world, although coverage is patchy in comparison with cellular.

Most Wi-Fi location will not have any restrictions to access, but there will be some locations that may restrict access in one of the following ways:

- Through a login procedure to users with a registered account.
- Some require users to be registered guest of their facility.

- Other may require users to be a customer.
- There are those that require a purchase to gain a password required to login.
- Some may ask some survey questions as part of a login process.

The Wi-Fi wireless broadband Internet connection allows users to do anything that one would do at home or the office on the Internet. Users can freely surf on the web, check and send e-mails, connect to your corporate network, make free voice over IP phone calls, play online games, update your blog, and IM with your friends.

4.2 Access Point

Access point consists of a radio transmitter and receiver as well as an interface to a wide network or directly to the network server as a base station and acts as bridge between the wireless network and a larger Ethernet network or the Internet.

4.3 Service Set IDentifier

Service Set IDentifier (SSID) is public name of WLAN. All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSID is set on the access point and broadcast to all wireless devices in range. It is case sensitive, consists of a sequence of alphanumeric character, and has a maximum length of 32 characters.

4.4 Access Point Authentication

Access Point Authentication comprises:

- Open Authentication, which does not do any checks on the identity of the station. The access point allows any station to join the network and shared authentication. Based on the challenge response system.
- Stations share a secret key.

5. STANDARDS

The IEEE 802.11 standard is actually only the earliest standard, allowing 1-2 Mbps of bandwidth. Amendments have be made to the original standard to optimise bandwidth (these include the 802.11a, 802.11b and 802.11g standards, which are called 802.11 physical standards) or to better specify components to ensure improved security or compatibility[3].

802.11a: The 802.11a standard (called Wi-Fi 5) allows higher bandwidth (54 Mbps maximum throughput, 30 Mbps in practice). The 802.11a standard provides eight radio channels in the 5 GHz frequency band.

802.11b: The 802.11b standard is currently the most widely used one. It offers a maximum throughput of 11 Mbps (6 Mbps in practice) and a reach of up to 300 m in an open environment. It uses the 2.4 GHz frequency range, with three radio channels available.

802.11c: The 802.11c bridging standard is of no interest to the general public. It is only an amended version of the 802.1d standard that lets 802.1d bridge with 802.11-compatible devices (on the data link level).

802.11d: The 802.11d standard is a supplement to the 802.11 standard and is meant to allow international use of local 802.11 networks. It lets different devices trade information on frequency ranges depending on what is permitted in the country where the device is from.

802.11e: The 802.11e standard is meant to improve the quality of service at the level of the *data link layer*. The standard's goal is to define the requirements of different packets in terms of bandwidth and transmission delay so as to allow better transmission of voice and video.

802.11f: The 802.11f is a recommendation for access point vendors that allow products to be more compatible. It uses the *Inter-Access Point Roaming Protocol*, which lets a roaming user transparently switch from one access point to another while moving around, no matter what brands of access points are used on the network infrastructure. This ability is also simply called *roaming.*

802.11g: The 802.11g standard offers high bandwidth (54 Mbps maximum throughput, 30 Mbps in practice) on the 2.4 GHz frequency range. The 802.11g standard is backwards-compatible with the 802.11b standard, meaning that devices that support the 802.11g standard can also work with 802.11b.

802.11h: The 802.11h standard is intended to bring together the 802.11 standard and the European standard (HiperLAN 2, hence the *h* in 802.11h) while conforming to European regulations related to frequency use and energy efficiency.

802.11i: The 802.11i standard is meant to improve the security of data transfers (by managing and distributing keys, and implementing encryption and authentication). This standard is based on the *AES* (Advanced Encryption Standard) and can encrypt transmissions that run on 802.11a, 802.11b and 802.11g technologies.

802.11j: The 802.11j standard is to Japanese regulation what the 802.11h is to European regulation.

802.11r: The 802.11r standard has been elaborated so

that it may use infra-red signals. This standard has become technologically obsolete.

6. SECURITY MEASURES

To prevent intercepting data by others the designers implemented many security techniques, like Wi-Fi Protected Access (based on encryption), Virtual Private Network (making virtual "tunnels"), Media Access Control Filtering (rejecting unknown MAC addresses), RADIUS Authentication and Authorisation (using login and password) or Kerberos (key distribution). There is also a possibility to combine some of these security mechanisms making the transmissions even more secure.

On the other hand providing such security in public places (like Internet cafes) may not meet its expectations. Connecting to the protected wireless network, security code, encryption key or a password is asked. If the code/key/password is not provided, it will not be able to establish a communication link and use Internet resources. Most of public areas do not use security modules because of that reason making Wi-Fi users data unsafe.

The "open air" nature of wireless radio signals poses challenges for securing wireless computer networks. No computer network is truly secure, but how does wireless network security stack up to that of traditional wired networks?

The following techniques can be implementing to serve wireless network.

- Antivirus software.
- Intrusion and detection system.
- Vulnerability assessment tools.
- Wireless firewall gateway.
- Personal firewall.
- Content filtering.
- Hard drive encryption.

Security is a big concern in wireless networking, especially in m-commerce and e-commerce applications. Mobility of users increases the security concerns in a wireless network. Current wireless networks employ authentication and data encryption techniques on the air interface to provide security to its users. The IEEE 801.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. In large enterprises, an IP network level security solution could ensure safety of corporate network and proprietary data. Virtual private network (VPN) is an option to make access to fixed access networks reliable. Since hackers are getting smarter, it is imperative that wireless security features must be updated constantly[4].

7. ADVANTAGES AND DISADVANTAGES

The Wi-Fi LAN has a broad application nowadays. Because of the comfortable and quick installation, people often replace old wired LANs with Wi-Fi. Such connection allows moving machine around the place without losing the Internet or other network resources. Some highly attended places like airports, libraries, schools or even coffee bars offer constant Internet connection using wireless LAN, so retrieving new files, cruising the global network or corresponding with others is not be a problem in those (and many other) places.

The most important shortcoming in Wi-Fi is the range. There may be difficulties in making a connection with a receiver which is 50-75 m away (inside the buildings). The signal should be stronger to provide larger connectable spaces. Additionally, some of the wireless adapters work on the frequencies that are currently used by many other wireless devices. It can cause a serious interference, so the connection performance can be quite poor.

However, building Wi-Fi network is often the cheapest way to achieve the desired connection with the surroundings. The price of a single wireless adapter is decreasing almost every day, so making a large network area by means of Wi-Fi is the most reasonable way. By the way, most of the Wi-Fi adapters have user-friendly configuration and diagnostic tools which can help to adjust or change WLAN settings or even can do everything for users.

7.1 Advantages

- Wi-Fi uses unlicensed radio spectrum and does not require regulatory approval for individual deployers.
- It allows LANs to be set up with cabling. It can reduce associated costs of network connection and expansions. Places where cables cannot be run, such as outdoor areas and historical buildings can use wireless LANs.
- Wi-Fi products are easily available in the market. There are different brands of access points and user's network interfaces are able to inter-operate at a very basic service level.

- Prices are considerably lower as competition amongst vendors has increased.
- Wi-Fi networks can support roaming. This allows mobile users with laptop to be able to move from one access point to another.
- Numerous access points and network interfaces support various degrees of encryption to protect traffic from interception.
- Wi-Fi has a set of global standards. Not like the cellular carriers, the same Wi-Fi users can work in different countries around the world at all time.

7.2 Disadvantages

Wi-Fi is still relatively new, there are following disadvantages too.

- The use of Wi-Fi band that is 2.4 GHz does not require a license in most countries provided that stays below limit of 100 mW and one accepts interference from other sources; including interference which causes the users devices to no longer function.
- The spectrum assignments and operational limitations are not consistent worldwide.
- Power consumption is fairly high compared to some other standards, making the battery life and heat a concern to some users.
- Wi-Fi uses the unlicensed 2.4 GHz spectrum, which often crowd with other devices such as Bluetooth, microwave ovens, cordless phones, or video sender devices, and many others. This may cause degradation in performance.
- Wi-Fi networks have limited range. A typical Wi-Fi home router might have a range of 45 m (150 ft) indoors and 90 m (300 ft) outdoors. Ranges may also vary as Wi-Fi is no exception to the physics of radio wave propagation with frequency band.
- The most common wireless encryption standard, wired equivalent privacy or WEP has been shown to be breakable even when it has been correctly configured.
- Access points could be used to steal personal and confidential information transmitted from Wi-Fi consumers.
- Intervention of a closed or encrypted access point with other open access points on the same or a nearby channel can prevent access to the open access points by others in the area. It poses a high problem in high-density areas such as large apartment blocks where many residents are operating Wi-Fi access points.
- Inter-operability issues between brands or deviations can cause limited connection or lower output speeds.
- Free access points can be used by the malicious to anonymous to initiate an attack that would be extremely difficult to track beyond the owner of the access point.

8. THE FUTURE

Wireless LAN technologies still have a long way to go. Both fundamental and practical problems still persist in this area. Therefore, it may be crucial to develop innovative and commercially viable solutions to some of the key issues and challenges discussed in this article to ensure the success of emerging wireless applications. The outlook of Wi-Fi broadband wireless Internet is boundless. The future is set to provide greater and longer connection ranges with faster transfer speeds. This allows users to freely surf on the web, check and send e-mails, connect to their corporate network, make free voice over IP phone calls, play online games, update their blogs, and IM with their friends more efficiently with stabilities. The future is set with many companies looking into offering users Wi-Fi not only around Internet cafes, coffee houses/shops, and airports around the world but also in public libraries, academic locations such as schools, colleges and universities, hotels, motels, resorts, apartment blocks, shopping centres, restaurants and even into homes and offices. This hopes to eliminate the hassles of dial-up Internet services and the fuss of costly installations of broadband cables, and broadband ADSL connections. With Wi-Fi available, consumers can freely use their computer around places where it suits them without all the lines and cables.

In the future, there will be better securities measures in protecting personal and confidential data's being received and sent out. There will also be better anti-virus and firewall protections whilst using Wi-Fi around destinated areas. With fierce competition of different companies, there would be cheaper Internet connection costs and choices for better services to consumers.

9. RECENT TRENDS OF WIRELESS TECHNOLOGY: WIMAX

WiMAX (World interoperability for Microwave Access) is a wireless technology mainly designed for bridging the last mile to the end user and providing him

with a broadband connection. WiMAX is based on standards developed by IEEE and ETSI, notably the IEEE 802.16 range of standards and the HIPERMAN standards. WiMAX can be used in different frequency bands in the range 2-66 GHz. It is claimed to be useful for urban, suburban and rural areas, sometimes with a non line of sight condition between base station antenna and subscriber station antenna. Intel has announced that they will start building WiMAX chipsets into laptop computers already in 2006.

WiMAX is not to be confused with Wi-Fi. The former is a metropolitan area networking technology whereas the latter is designed for local area networking. With WiMAX, nomadic users can be served, for instance, while they are stationary or when they have a walk during a communications session. A WiMAX area served by one base station is termed “Hot zone” because it is considerably larger than a Wi-Fi service area called “Hot spot”.

WiMAX can provide broadband wireless access (BWA) up to 30 miles (50 km) for fixed stations, and 3 - 10 miles (5 - 15 km) for mobile stations. In contrast, the Wi-Fi/802.11 wireless local area network standard is limited in most cases to only 100-300 feet (30-100m). With WiMAX, Wi-Fi-like data rates are easily supported, but the issue of interference is lessened. WiMAX operates on both licensed and non-licensed frequencies, providing a regulated environment and viable economic model for wireless carriers. WiMAX can be used for wireless networking in much the same way as the more common Wi-Fi protocol. WiMAX is a second-generation protocol that allows for more efficient bandwidth use, interference avoidance, and is intended to allow higher data rates over longer distances. The IEEE 802.16 family of standards and its associated industry consortium, WiMax, promise to deliver high data rates over large areas to a large number of users in the near future. This exciting addition to current broadband options such as DSL, cable, and Wi-Fi promises to rapidly provide broadband access to locations in the world’s rural and developing areas where broadband is currently unavailable, as well as competing for urban market share. WiMax’s competitiveness in the marketplace largely depends on the actual data rates and ranges that are achieved, but this has been difficult to judge due to the large number of possible options and competing marketing claims[5].

9.1 Technical Characteristics

WiMAX is based on well-designed and thoroughly calculated standards, contrary to e.g. Wi-Fi. In the physical layer, OFDM (Orthogonal Frequency Division Multiplexing) is applied in the 2-11 GHz frequency range, which makes WiMAX signals resistant to multipath effect and selective fading. The standards have means to provide quality of service (QoS) guarantees, which is extremely important for real-time services such as telephony. Security issues are treated by authentication and encryption mechanisms. WiMAX is usable in both licensed frequency bands and licence exempt bands. The most important frequency bands for WiMAX usage in Europe will be the 3.5 GHz and 5 GHz bands.

The system design encompass advanced concepts such as adaptive modulation where the system is able to apply different modulation methods depending on the communication link signal to noise ratio. Spatial diversity techniques and adaptive antenna systems are available to the WiMAX system designer. This enables signals from multiple antenna elements to be coherently combined to concentrate the transmission or reception to a particular direction or directions. Mesh networking is an interesting feature where a subscriber station is able to relay signals to and from other stations that do not have a direct contact to the base station. With this, the range can be extended and coverage holes be filled.

9.2 Usage

WiMAX will be used in urban, suburban and rural areas, particularly where other broadband means are not available or installations are expensive. Competition to DSL will not be fierce in areas where it is already established due to its relatively low costs and high penetration. Furthermore, a high density of WiMAX base stations will be needed in urban and suburban areas to serve customers with self-installable CPE and reasonable data rates. In fact, the cell sizes under these conditions are only a few hundred metres. WiMAX is likely to play an important role in serving rural areas. There, cell sizes of 5-10 km are possible requiring outdoor antennas at the customer premises. The speed can be increased by strengthening the signals. For a fixed transmitting power and antenna gain, this means lower range. Thus, ranges are lower if more speed is desired, e.g., for 26 Mb/s the 1-2 km range for terrain type B would drop down to 700 m[6].

10. WI-FI AT INDIAN STATISTICAL INSTITUTE, BENGALURU CENTRE

The use of Wi-Fi at the Indian Statistical Institute (ISI) has been active since 2004. In 2004, ISIBC started implementing the WLAN stage-by-stage. By the end of 2009 the WLAN has covered almost all the blocks of the building in the Campus including Faculty Blocks, Administration Blocks, Students Labs, Students Hostels, Gust Houses, Auditoriums, etc. The network architecture at ISI is shown in Fig. 1.

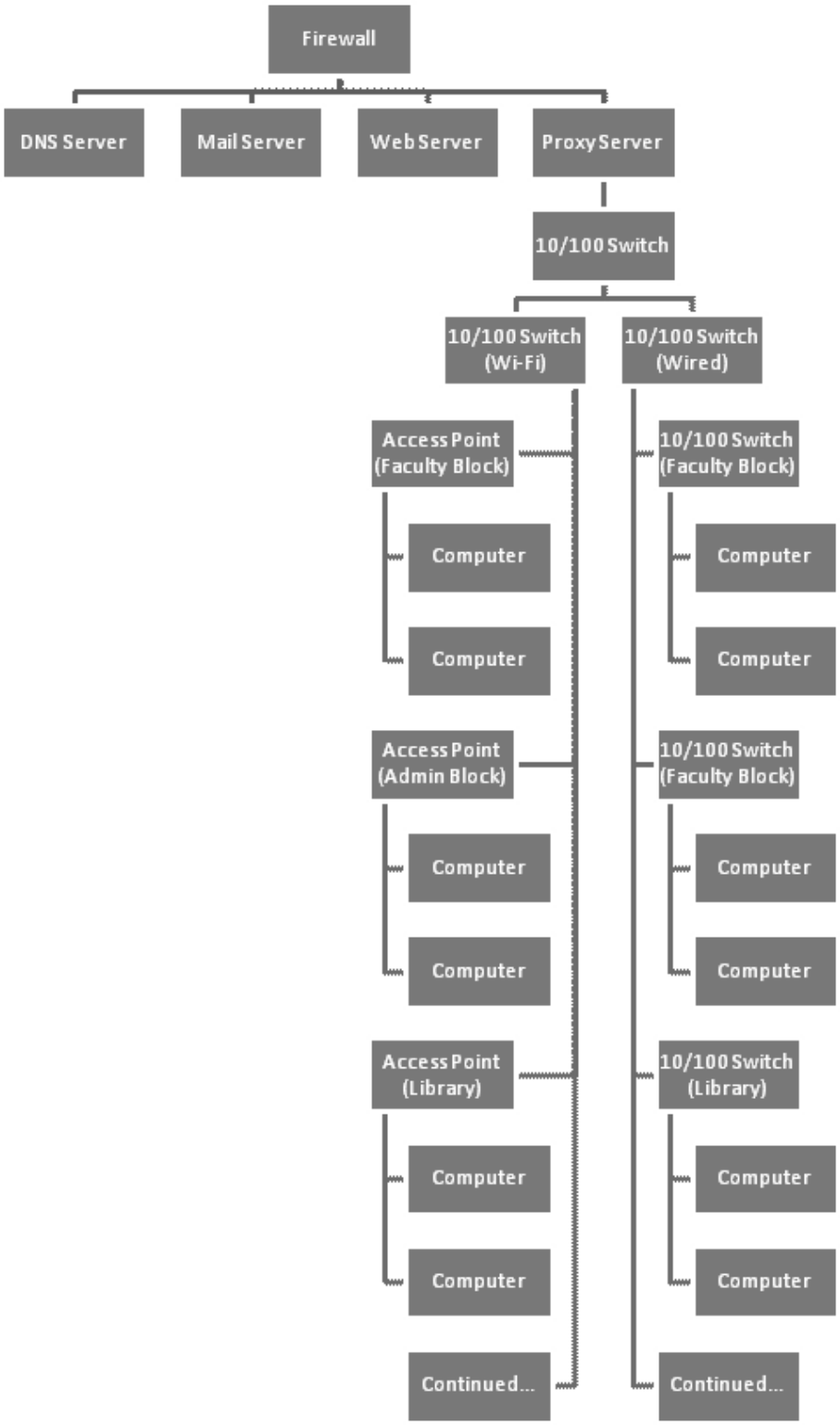

Figure 1. Network architecture (Wi-Fi+wired) at ISI, Bengaluru.

10.1 Applications

The state-of-the-art facility of the WLAN at the Institute has strengthened the use of the Internet and Intranet services of the Institute very effectively. Every user and visitor of the Institute can use the WLAN facility provided with proper access key. The Library has been facilitated with the applications such as Libsys, OPAC and Web OPAC, dspace, etc. Users can access the information/data available in the Library through WLAN.

10.2 LAN Topology

Network topology is defined as the physical interconnection of the various elements (links, nodes, etc.) of a computer network. Network topologies can be physical or logical. Physical topology means the physical design of a network including the devices, location and cable installation. Logical topology refers to the fact that how data actually transfers in a network as opposed to its design.

Topology can be considered as a virtual shape or structure of a network. This shape actually does not correspond to the actual physical design of the devices on the computer network. The computers on the home network can be arranged in a circle shape but it does not necessarily mean that it presents a ring topology.

Hybrid networks use a combination of any two or more topologies in such a way that the resulting network does not exhibit one of the standard topologies (e.g., bus, star, ring, etc.). For example, a tree network connected to a tree network is still a tree network, but two star networks connected together exhibit a hybrid network topology. A hybrid topology is always produced when two different basic network topologies are connected.

Two common examples for hybrid network are: Star Ring Network and Star Bus Network. A Star Ring Network consists of two or more star topologies connected using a multi-station access unit (MAU) as a centralised hub. A Star Bus Network consists of two or more star topologies connected using a bus trunk (the bus trunk serves as the network's backbone)

The Star Bus Network topology has been adopted at Indian Statistical Institute, Bengaluru where the Library computers have been connected to serve the users using Wi-Fi or Wired.

11. CONCLUSION

The use of Wi-Fi technology at ISI, Bengaluru libraries can be rated as relatively good. Users access the information from the departments, hostels and computer centres and also from the libraries. Wi-Fi technology has highlighted the importance of achieving capability among databases and information products, hardware and software, input formats, processing, data exchange, output formats has to be address. Its main focus is utilising the resource in a productive manner. We are witnessing today the emergence of global network infrastructure, wherein WLAN are rapidly getting interconnected.

REFERENCES

1. Neelameghan, A. & Chester, Greg. Knowledge management in relation to indigenous and marginalized communities in the digital era. *Information Studies*, 2007, **13**(2), 73-06.

2. Nardi, Bonnie. A social ecology of wireless technology, 2003, **8**(8). http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1069 (accessed on 28 April 2010).

3. IEEE 802.11Std, 1999.

4. Chandramouli, R & Subbalakshmi, K.P. Wireless LAN: Issues and challenges. *Ticker,* 2001.

5. Ghosh, Arunabha; Wolter, David R; Andrews, Jeffrey G. & Chen, Runhua. Broadband wireless access with WiMax/802.16: Current performance benchmarks and future potential. *IEEE Commun. Mag.*, 2005, **43**(2), 129-36.

6. Saemundur, E & Thorsteinsson, Síminn. The significance of WiMax. http://www.eurescom.eu/message/messageMar2005/The_significance_of_WiMAX_Eurescom_Study_WiBAN.asp. (accessed on 11 Jan 2010).