WIRELESS LAN AND IEEE 802.11 IN DIGITAL LIBRARY

ASHISH KR SRIVASTAVA **JAY SINGH**

SANJAY KR DIWAKAR

Abstract

We seem to recall a time when protocols and standards were two different things. In the past couple of years, the craze over new protocols has seemingly breathed new life into library information technology, replacing the doldrums of standards with the hope of new, universally accepted protocols. We must admit to being too young to have been there, but we wonder if things felt like this when MARC and Wireless LAN were poised to change the world of library automation as also in XML, OpenURL, and the Open Archives. An increased rate of mobility brought about by the Wireless LAN break through has given a new dimension to networking capabilities. The IEEE 802.11 defines standards for both 1-2 Mbps and higher speed wireless communication. The study of the PHY and the MAC layer as per the IEEE 802.11 protocols reveal that the issues like security and reliability of utmost importance in this type of networking. In short if higher speed networking of this kind can be created then there would be no need for the conventional physical medium communication. Globalization of this technology would indeed bring the world closer and bring about a new era of wireless technology in the Library.

Keywords : Wireless LAN/ IEEE 802.11/ Wireless communication/ Digital Library/ Physical layer/ MAC layer

1. Introduction

LANs or Local area networks have become a core part of communication in today's world. Every business environment has a LAN technology to connect its terminals hence serving as a platform for data communication. Technology enhancements today, bring improvements in the networking world in the form of faster, reliable and secure LANs. The latest business and household needs demand for a technology that would destroy the physical medium barrier and step into a world of mobile communication. Thousands of people over the face of this earth today already savor the fruits of mobile communication, through cellular phones, pagers and other messaging media. Thus the need arises to merge the mobile technology to the realm of personal and business computing. Hence the attractive concept of wireless LAN or WLAN comes into picture. A diagrammatic representation of WLAN is shown in Figure 1.

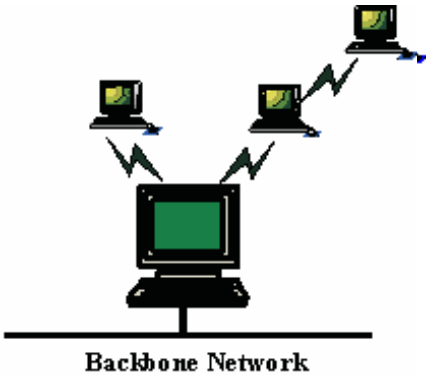


Figure 1

2. The Emergence

The evolution of data communication since Ethernet project in the early 1970's has been extensive. High speed LANs, with cheap hardware is being used in almost every business and personal domain but some network users especially those in the field of medicine, business and universities would be better served if phone dial-ups, network nodes were not limited to access through wired, land line connections. There were several needs and advantages that prompted mobile computing:

Need for mobility

Users of the network are now not restricted to the bounds of there homes or work areas. They can use mobile computing devices (laptop computers, hand-held computers, etc.) to access information from any environment and during any time. Particularly there is use when conducting business meetings and conferences where the network established needs to be torn down in a very small amount of time. Traders at the stock exchange use wireless to conduct trading. Students too can now access the course materials on the network while anywhere on the campus.

Security

Security while using voice terminals is much higher than those using fixed terminals like the PC. This is because of the use of Internet enabled terminals as Personal Trusted Devices (PTDs) to conduct diverse mobile ecommerce transactions and also their extensive usage in the cooperate world. All this makes fixed terminals more susceptible to thefts. Information stored on these terminals can fall in the hands of wrong kinds of people who may have criminal or competitive intentions. .

Real-time applications

Wireless networking is applicable to all business and industries where there is a need for real time access to information and incases where installation of a physical media

is not feasible. Such networking is especially useful when employees must process information on the spot, directly in front of customers, via electronic-based forms and interactive menus. Some areas where such a need arises are in the field of medicine where doctors can monitor the patient's vital signs without physical presence and electronic terminal. Factory floor workers can access part and process specifications without impractical or impossible wired network connections. Further inventory control can be done effectively with the help of wireless scanners. Merchants can use wireless "smart" price tags, complete with Liquid Crystal Display (LCD) readouts to eliminate discrepancies between stock-point pricing and scanned prices during checkout.

Information processing

When coupled with centralized databases, wireless connections can meet with mobility needs, while eliminating paperwork, reducing errors, cost and improving overall efficiency. The alternative to this, which many companies still employ, is utilizing paperwork to update records, process inventories, and file claims. This manual method processes information slowly, produces redundant data, and is subject to errors caused by illegible handwriting.

Cost effectiveness

Finally using WLAN can be cost effective in instances where the cost involved in the maintenance of old buildings is higher than installing WLAN. WLANs offer the connectivity and the convenience of wired LANs without the need for expensive wiring or rewiring. Currently WLANs with speed up to 2 Mbps has been created. Some companies are working to create WLANs that will have speed of 11Mbps.

3. How it all Works

WLANs use radio or infrared (electromagnetic airwaves) to transmit data from one point to another without any physical connection. These airwaves are the carriers that deliver energy to the remote recipient of the data. The data being transmitted is superimposed (modulated) on these radio carriers so that it can be accurately extracted at the receiving end. The modulated signal occupies more than a single frequency, since the frequency or bit rate of the modulating information adds to the carrier. Each frequency band can have more than one carrier without interfering. Various signal-spread schemes are used at the physical layer to facilitate this. In WLAN architecture, a transceiver, called as An Access Point, connects to the wired network from a fixed location using standard cabling. The access point can receive, store and transmit data between the WLAN and the wired network infrastructure. A single access point can support a small group of users and can function within a range of less than one hundred to several hundred feet. The access point is usually mounted high but may be mounted essentially anywhere that is practical as long as the desired radio coverage is obtained. End users access the network through WLAN adapters, which are implemented as PCMC cards in notebook or palmtop computers, as cards in desktop computers, or integrated within hand-held computers. WLAN adapters provide an interface between the client network

operating system (NOS) and the airwaves via an antenna. The nature of the wireless connection is transparent to the NOS.

IEEE 802.11 The IEEE has established two standards for WLAN technology. This standard is described as the 802.11 workforce. The IEEE 802.11 protocol describes the physical and the MAC layer. This working group describes the WLAN having a maximum speed of 2Mbps. There are other workforces like **Task Group a** and **Task Group b** that will work on future advancements in the WLAN technology. The following tables enlist the properties of the various workforces.

IEEE 802.11
Developing a PHY in the 2.4 GHz frequency band. Data rate is 1-2 Mbps. Used for wireless Ethernet (LAN)

Task Group a
Developing a PHY in the 5 GHz ISM band. It supports voice as well as images as data. Data rate is 20-25 Mbps. Used for Wireless (ATM).

Task Group b
Developing a PHY in the 2.4 GHz frequency band. There is backward compatible with existing products. It supports computation of higher data rates. LAN speed is 11 Mbps Used for wireless Ethernet (LAN)

3.1 IEEE WLAN Architecture

The 802.11 architecture consists of various components that are highly abstracted to the higher layers of the network stack. .

WLAN Station

The station (STA) is the most basic component of the wireless network. It is a device that provides the MAC, PHY and connection functionality to the network. They provide services like authentication, de-authentication, privacy, and data delivery. Examples of stations are laptop PCs, handheld devices, or Access Points. Stations can be mobile, portable, or stationary. .

Basic Service Set

The Basic Service Set (BSS) is the building block of an 802.11 WLAN. The BSS consists of a group of any number of stations.

4. Topologies

The IEEE proposes two architectural simulation of the WLAN: Ad-hoc and infrastructure architecture. The two are studied as follows:

Ad-hoc

Here the networks to be connected are brought together as a mesh. Here all the mobile stations communicate directly with each other. Every mobile station may not be able to communicate with every other station due to the range limitations. There are no relay functions in an IBSS therefore all stations need to be within range of each other and communicate directly. An analogy used can be a conference where each delegate brings a laptop to discuss matters. Here the trend is to elect one machine as a master or base station and the others as slaves to settle the spokesman issue. Flooding and broadcast between nodes can also be used to identify all the nodes in the network. This type is also known as Independent Basic Service Set (IBSS). Figure 2 shows ad-hoc network architecture.

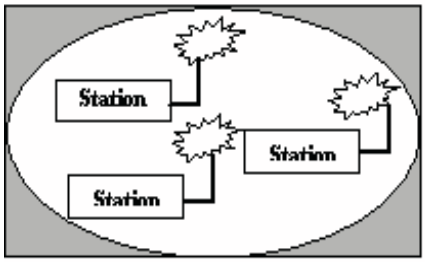


Figure 2

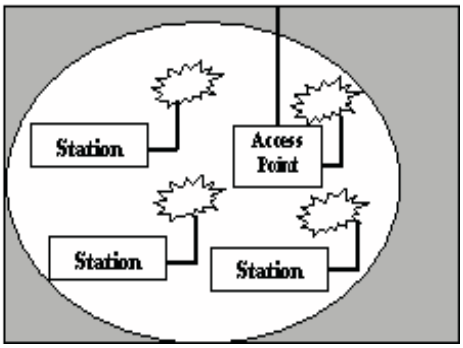


Figure 3

Here the architecture requires the fixed access points with which the nodes can communicate. The access point provides a local relay function for the BSS. This structure is very similar to the present day cellular networks around the world. The access point provides a local relay function for the BSS. All stations in the BSS communicate through the access points and not directly. All frames are relayed between stations by the access point. The access point may also provide connection to a Distribution System (DS). It is the means by which an access point communicates with another access point to exchange frames for stations in their respective BSSs, forward frames to follow mobile stations as they move from one BSS to another, and exchange frames with a wired network. Figure 3 shows the network architecture.

The Figure 4 shows the schematic representation of the architecture

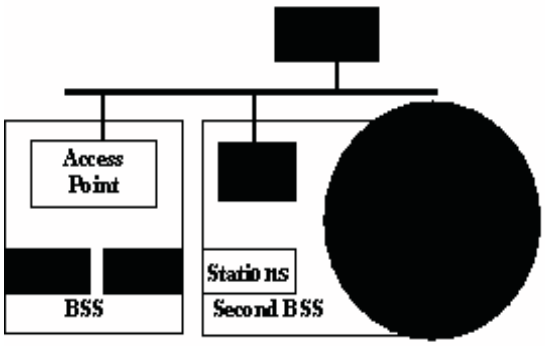


Figure 4

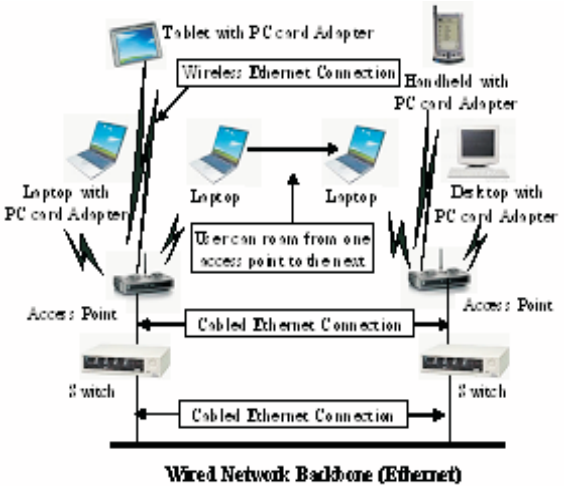


Figure 5

The Figure 5 shows a diagrammatic representation of the architecture.

4.1 Physical Layer

The physical layer handles the actual node to- node transmission of data. Here the physical layer is divided into 2 Sublayers namely the Physical Layer Convergence Procedure (PLCP) Sublayer and the Physical Media Dependent (PMD) Sublayer. The Figure 6 shows the sublayers of the physical layer.

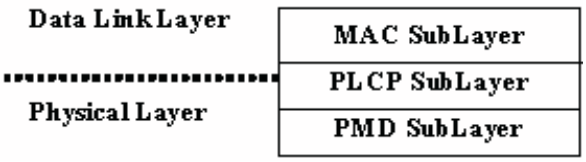


Figure 6

- **PLCP** This Sublayer plays the role of a physical medium dependent system to the Physical layer. It forms a mapping for the PSDU (Physical layer Service Data Unit) into a framing format that is used between stations that actually use the physical medium to transmit and send data. This facilitates the MAC layer to work with maximum efficiency.

- **PMD** It provides a clear channel assessment mechanism and defines the characteristics and method of transmitting and receiving data through a wireless medium between two or more stations each using the same modulation system. The IEEE 802.11 standard specifies three types of PHY-two them, FHSS and DSSS are RF and the third is Infrared.

- **Frequency Hopping Spread Spectrum (FHSS)** Here the data signal is taken and modulated with a carrier signal that hops from frequency to frequency as a function of time over a wide band of frequencies. With frequency hopping spread spectrum, the carrier frequency changes periodically. The frequency hopping technique reduces interference because an interfering signal from a narrowband system will only affect the spread spectrum signal if both are transmitting at the same frequency at the same time. Thus, the aggregate interference will be very low, resulting in little or no bit errors. A frequency hopping radio, for example, will hop the carrier frequency over the 2.4 GHz frequency band between 2.4 GHz and 2.483 GHz. Figure 7 illustrates the above method

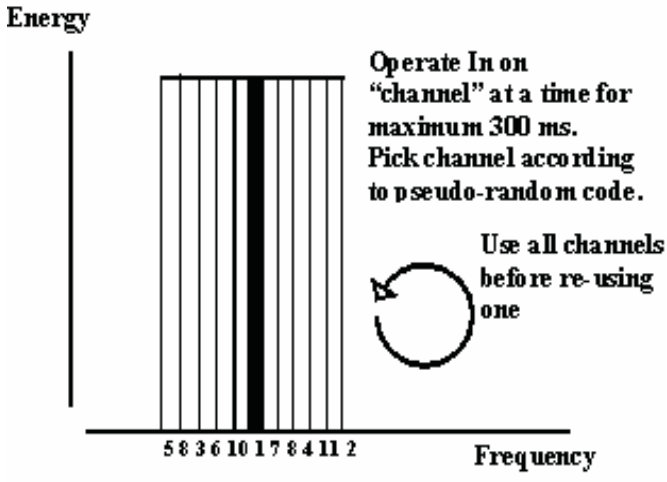


Figure 7

- **Direct Sequence Spread Spectrum (DSSS)** Here the data signal is combined at the sending station with a higher data rate bit sequence, which many refer to as a chipping code. A high chipping code increases the signals resistance to interference. The minimum linear processing gain that the FCC allows is 10, and most commercial products operate under 20. The IEEE 802.11 Working Group has set their minimum processing gain requirements at 11. In comparison to frequency hopping, direct sequence can achieve much higher than 2 Mbps data rates. Figure 8 illustrates the above method.

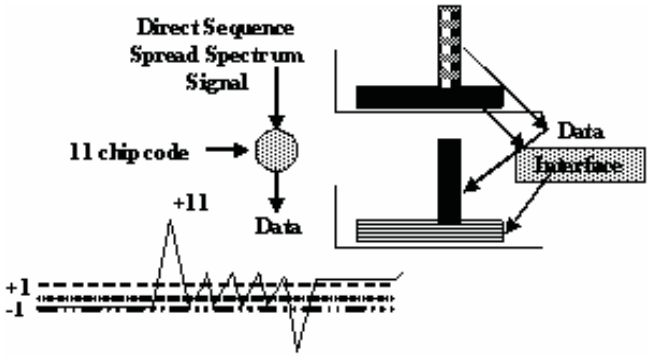


Figure 8

- **InfraRed (IR)** Here the system uses very high frequencies, just below visible light in the electromagnetic spectrum, to carry data. Like light, IR cannot penetrate opaque objects; it is either directed (line-of-sight) or diffuse technology. Inexpensive directed systems provide very limited range (3 ft) and typically are used for personal area networks but occasionally are used in specific WLAN applications. High performance directed IR is impractical for mobile users and is therefore used only to implement fixed sub-networks. Diffuse (or reflective) IR WLAN systems do not require line-of-sight, but cells are limited to individual rooms. This method is considered relatively secure. The infrared physical layer specifies 4 and 16 level pulse position modulation (PPM) operating at 850-950 nM at 1 and 2MBPS. To summarize the above we can differentiate between the Frequency Hopping and Direct Sequence:

FREQUENCY HOPPING	DIRECT SEQUENCE
• Simple modulation (FSK)	• Efficient modulation (PSK)
• .Narrowband, discontinuous transmission	• Broad modulation bandwidth, continuous transmission
• .More network overhead	• Quick synchronization
• Higher power density can generate interference	• Low power density minimizes interference

There are other twp types that are used in high speed WLAN. IEEE 802.11a specifies OFDM and IEEE 802.11b specifies HR/DSSS. .

- **High Rate Direct Sequence Spread Spectrum (HR/DSSS)** This is Direct Sequence Spread Spectrum implemented at a higher frequency. .

- **Orthogonal Frequency Division Multiplexing (OFDM)** Orthogonal Frequency Division Multiplexing (OFDM) is a method of transmitting data by dividing the stream into several parallel bit streams, each of which has a much lower bit rate,

where these substreams are used to modulate several carriers. In OFDM time-domain waveforms are chosen such that mutual orthogonality is ensured even though subcarrier spectra may overlap. It appeared that such waveforms could be generated using a Fast Fourier Transform at the transmitter and receiver.

4.2 MAC Layer

All the three physical layers described above, operate with a common MAC layer to co-ordinate the traffic over the medium. The physical layer senses the RF medium using a received signal strength indication (RSSI) and carrier sense. The MAC and physical layer use these indicators to determine if the channel is clear to transmit. This is controlled by the CCA - clear channel assessment algorithm embedded in the physical layer.

MAC protocol

IEEE 802.11 specifies the CSMA/CA i.e. Carrier Sense Multiple Access/ Collision Avoidance protocol for multi-access collision avoidance. Here the packet is sent across the channel by the sender only if there is no other node transmitting its packet. If there is contention then there is a back off algorithm that calculates the amount of time the node must wait before it tries re-transmission. Collision is minimized here because of the nature of the back off algorithm that ensures that two contending nodes have a very less probability of having the same time interval before retransmission. Collision detection defers from that of Ethernet as here the sending node cannot get signals from other nodes sending packets has its own signal overrides all the other signals.

Handshake signals

Whenever a node is ready to transmit, it sends out a brief ready-to-send (RTS) packet that will have the length information of the packet to be transmitted. The Receiving node in acknowledgement sends a clear-to-send (CTS). Then the packet transmission occurs. The receiver will then perform a CRC check on the packet. If it is successfully received then an acknowledgement (ACK) is sent to the sender.

Hidden node problem and its solution

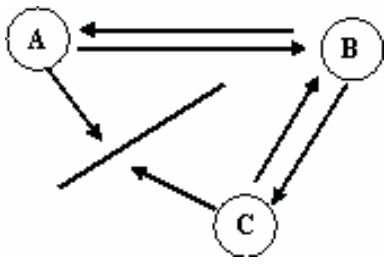


Figure 9

- **The Problem** Consider the Figure 9Here node A can communicate with node B, and node B can communicate with node C. But node A cannot communicate node C. Thus although node A may sense the channel to be clear, node C may in fact be transmitting to node B. Thus resulting in a collision.

- **The solution** The handshake signals RTS and CTS protect against hidden-station interference. All 802.11 receivers must support RTS/CTS, but support is optional in transmitters. Here node A is alerted that node B is busy and thus node A waits before it transmits.

Services provided by the MAC

- **Client Authentication and Privacy** Authentication is a network management function that restricts network access to unauthorized clients. A special RTS/ CTS control frame is used to authenticate users over the network. There are two kinds of authentication - Open and Shared Key.

  - Open authentication: This allows multiple clients to associate with access points in a given area without identifying the user. The node asking for authentication first sends a frame identifying itself. The other node will then alert the sender if its authentication has been established or not.

  - Shared Key authentication: This type of authentication assumes that each station has obtained a secret shared key through a secure channel independent of the 802.11 network. Stations authenticate through shared knowledge of the secret key. This type of authentication uses WEP - wired equivalent privacy - to secure the WLAN system. Access point and clients are configured using a shared encryption key. WEP adds a level of privacy and security to control access to the network.

- **Power Management** The MAC layer specifies two modes of power management for those applications requiring mobility under battery operation namely, Active Mode and Power Save Mode. The active mode indicates that the client is powered to transmit and receive information. Power save mode indicates that the client is in an inactive sleep state and unable to transmit or receive information. .

- **Roaming** Roaming is a feature supported by the MAC layer. This allows multiple adjoining basic service areas to extend the coverage area. The feature allows clients to associate and re-associate with multiple access points with a common ESSID (wireless network segment identifier).

- **Privacy** Due to the privacy violation issues that are encountered in a wireless transmission, a privacy service is applied to all data frames and some authentication management frames. This is done with the help of the 802.11 Wired Equivalent Privacy (WEP) algorithms. In addition to the above the MAC layer most importantly ensures reliable transmission of data with minimum duplication and reordering of frames. This service is known as the Data delivery service.

The Wired Equivalent Privacy (WEP) algorithm

The Wired Equivalent Privacy (WEP) protocol is used to protect link layer communication from eavesdropping and other attacks. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security we find in a wired medium.

Attributes of WEP

The WEP algorithm has following properties:

- **Reasonably strong** The algorithm has mechanisms to prevent the brute force attack used in any kind of violation of security. The algorithm frequently changes the secret key and also the length of the secret key.
- **Self-synchronizing** WEP is self-synchronizing for each message. This property is critical for a datalink level encryption algorithm, where "best effort" delivery is assumed and packet loss rates may be high.
- **Efficient** The WEP algorithm is efficient and may be implemented in either hardware or software.
- **Optional** The implementation and use of WEP is an IEEE 802.11 option.

Problems with WEP Certain problems encountered with the algorithm seriously undermine the security claims of the system. Figure 10 shows the types of attack the WEP is susceptible to.

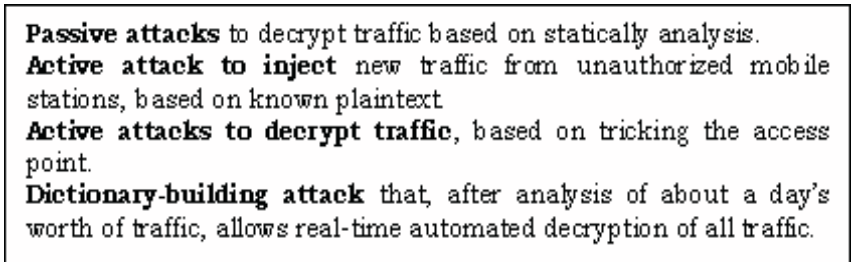


Figure: 10

4.3 The Network Layer

Mobile IP

Mobile IP draws attention at the network layer. Here IP address of the mobile machine does not change when it moves and a forwarding mechanism is used to maintain connection to the network. The analogy used to explain the concept is that of a person who when changes his residence lets his local post office know about the name of their

new post office. When he actually shifts, he registers with the new post office. All his mails know will be forwarded from his old to new post office. Similarly all packets are forwarded from the mobile agents local IP to new agent's IP on the new network. When the mobile agent returns to its original network, it informs both agents (home and foreign) that the original configuration has been restored. No one on the outside networks need to know that the mobile agent moved. However in this whole process if the mobile agent is somewhere between it's local and new network, there is a requirement for storing of packets.

5. Drawbacks of WLAN

As the discussion for need for mobility and freedom from wired network continues there are some issues that need to be highlighted. There are some drawbacks of WLAN that need to be studied.

Rate of error

There are several more sources of error in wireless transmission as compared with to wired networks. Noise, multipath interferences, attenuation, spread-spectrum interference, etc. are all common causes for errors in wireless environments. Figure shows Multipath interferences caused by blockages like trees, terrain contours and man made structures. Figure 11 illustrates this problem

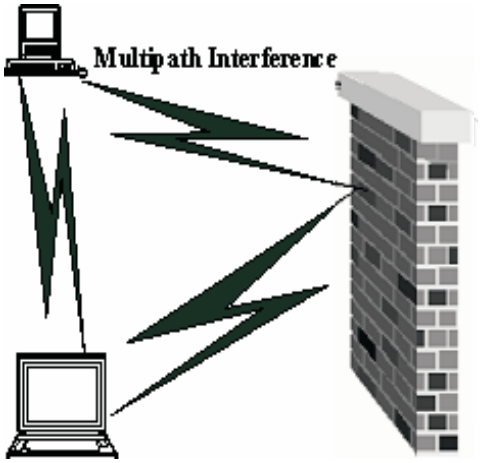


Figure 11

Security

There is a higher possibility of signals being eavesdropped and tampered with in a wireless network because there is no restricted domain for the signal path and hence lesser control over data. As discussed in the MAC layer, the issue of security and error rate are controlled by the help of certain service protocols.

Interference

Dye to lack of any connection there is a possibility of other network signals interfering with the network. Such an interfering signal could be that of a microwaves or cellular phones.

Power conservation

Wireless LANs are battery dependent as a power source that is costlier and scarcer than electricity as a power source.

5.1 Types of WLAN

Bluetooth and HomeRF are some WLAN technologies.

About Bluetooth Bluetooth is the technology specification for small form factor, low-cost, short-range radio links between mobile PCs, mobile phones and other portable devices. It uses a single 9x9mm chip, 2-way radio for high-speed communication. It enables portable electronic devices to communicate wirelessly via short-range ad hoc networks. Conceived initially by Ericsson, before being adopted by a myriad of other companies, Bluetooth chip is designed to replace cables by taking the information normally carried by the cable, and transmitting it at a special frequency to a receiver Bluetooth chip, which will then give the information received to the computer, phone whatever.

6. Conclusion

WLAN technology has changed the face of data communication system. There is no longer a need for physical medium for transmission and there is an increased rate in mobility. The 802.11 addresses issues like mobility, security, reliability, and the dynamic nature of WLAN as well as maintaining the basic network architecture. At present three broad applications can be serviced by including home control applications, voice/basic data applications, and multimedia applications. For home control applications data rates of approximately only 10 Kbps are required. For voice and basic data networking data rates of 1-2 Mbps are sufficient given that the majority of households will still be connecting to the Internet using dial-up connections. Moreover, throughput of 1-2 Mbps is sufficient to handle the effective speed most broadband services provide today. However, in order to stream video significantly higher data rates are needed. A DVD stream would require an effective throughput of 3-8 Mbps, while a HDTV stream would require an effective throughput of around 19 Mbps. For the immediate future wireless networking products must be able to achieve effective data rates of approximately 8 Mbps in order to realistically target multimedia applications.

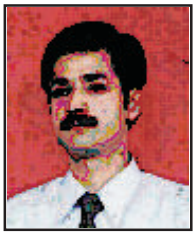
References

1. IEEE Computer Society's Student Newsletter; "A Short Tutorial on Wireless LANs and IEEE 802.11" at:http://www.computer.org/students/lo oking/summer97/ieee802.htm

2. Online article on: "Introduction to IEEE 802.11", at: http://www.intelligraphics.com/articl es/80211_article.html

3. White paper on WLAN at: http://www.d2d.com/white80211.html

BIOGRAPHY OF AUTHORS



Mr. Ashish Kumar Srivastava is Assistant Librarian at CSJM University, Kanpur.

Email: ashish.csjmu@gamil.com

Mr. Jay Singh is Lecturer at Department of Library & Information Science, CSJM University, Kanpur.

Email: singh1jay@yahoo.co.in

Mr. Sanjay K. Diwakar works as Information Scientist with Central Library of CSJM University, Kanpur – 208024. He has 4 years of experience in Computer Science. Actively involved in Software Development using J2EE Technologies. He has 3 years of teaching experience in Computer Science. Actively involved in Computer Science teaching at Kanpur University.

Email: skrd@iitk.ac.in