WI-FI TECHNOLOGY: SECURITY ISSUES

Vandana Wekhande*
Graduate student, M.S. in Computer Science Program, Rivier College

Keywords: *Wireless Internet,802.11b, Wi-Fi*

Abstract

Wi-Fi® is a system of wirelessly connecting devices that use radio waves, allowing for connection between devices without the expense of cumbersome cables or without needing them to be facing one another. Wi-Fi stands for Wireless Fidelity® and is used to define the wireless technology in the IEEE 802.11b standard. It operates in the unlicensed 2.4 GHz radio spectrum, uses direct-sequence spread-spectrum (DSSS) for modulation, supports variable data rates up to 11 Mbps, and has a range of about 50 meters.

Wi-Fi allows users to gain convenient wireless internet access, though without the sufficient security precautions it can also let outsiders or intruders to do the same without anyone noticing. As "hot-spots" are becoming increasingly popular and cities working towards becoming entirely wireless, users is becoming more vulnerable to cyber crime. Techno-criminal can attack a user's wireless network in order to gain free internet usage or obtain personal and valuable information.

The threat of intrusion into the home wireless network has forced users to adopt a range of security. Security measures have improved since the release of the first system called Wired Equivalent Privacy (WEP). The majority of new Wi-Fi products use a system called Wi-Fi Protected Access, created by the Wi-Fi Alliance. It not only provides a 128-bit encryption of data that is being transmitted but locks on to individual computers and changes the access key every 10000 packets. It is more complicated than WEP, though it is more secure with improved authentication, authorization and encryption capabilities.

Introduction

Wi-Fi is a system of wirelessly connecting devices that use radio waves, allowing for connection between devices without the expense of cumbersome cables or without needing them to be facing one another. Wireless local area networks (LANs) have achieved a tremendous amount of growth in recent years. Among various wireless LAN technologies, the IEEE 802.11b based wireless LAN technology, Wi-Fi, can be cited as the most prominent technology today.

The 802.11 index refers to a family of specifications developed by the IEEE for wireless LAN. The 802.11 specifies an over-the-air between a client and a base station or between two wireless clients. The IEEE accepted the specification in 1997.

There are several specifications in the 802.11 family:

- **802.11** – applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

- **802.11a** – an extension to 802.11 that applies to and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS.
- **802.11b** (also referred to as *802.11 High Rate* or Wi-Fi) – an extension to 802.11 that applies to wireless and provides 11 Mbps transmission (with a fallback to 5.5, 2.0, and 1.0 Mbps) in the 2.4 GHz band. The 802.11b uses only DSSS. It has been the 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to the Ethernet.
- **802.11g** – applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band.

There are many wireless LAN technologies nowadays, such as, Wi-Fi, Bluetooth, HiperLAN, HomeRF, etc. All these technologies operate in the 2.4-GHz ISM (Industrial, Scientific, and Medical) radio spectrum. Each technology has its own niche depending on the deployment requirements of the wireless LANs. The only technology, which has received the widest market acceptance, is IEEE 802.11b or Wi-Fi. The popularity of this standard is aptly reflected in portable computer vendors' decision to integrate 802.11b wireless network adapters with notebook computers.

1 Wi-Fi Technology Overview

1.1 Wi-Fi Technology Categories

Wi-Fi Technology falls into one of the following four categories [5]:

- **Infrared LANs** at 1 Mbps and 2 Mbps operates at a wavelength between 850 and 950 nm. An individual cell of an IR LAN is limited to a single room because infrared light does not penetrate opaque walls.
- **Direct-sequence spread spectrum** operates in the 2.4-GHz ISM band. Up to seven channels, each with a data rate of 1 Mbps and 2 Mbps can be used. In most cases, these LANs operate in the ISM (industrial, scientific, and medical) bands; therefore, no FCC licensing is required for use in the United States. Under the Direct-Sequence-Spread Spectrum each bit in the original signal is represented by multiple bits in the transmitted signal, known as a chipping code. The chipping code spreads the signal across a wider frequency band in direct proportion to the bits used. Therefore, a 10-bit chipping code spreads the signal across a frequency band that is 10 times greater than the 1-bit chipping code.
- **Frequency-hopping spread spectrum** operates in the 2.4-GHz ISM band, at data rates of 1 Mbps and 2 Mbps. In most cases, these LANs operate in the ISM (industrial, scientific, and medical) bands; therefore, no FCC licensing is required for use in the United States. Under Frequency-hopping the signal is broadcast over seemingly random series of radio frequencies, hopping from frequency to frequency at fixed intervals. A receiver, hopping between frequencies in synchronization with the transmitter, picks up the message. Would-be eaves-droppers hear only unintelligible blips. Attempts to jam the signal succeed only in knocking out a few bits.
- **Narrowband microwave LANs** operate at microwave frequencies, but do not use spread spectrum.

1.2 Wi-Fi IEEE 802.11 Services

There are five types of services for Wi-Fi IEEE802.11:

- **Association**: Establishes an initial association between a station and an access point within a particular BSS. The access point can then communicate information (station identity, its address) to other access points within the ESS to facilitate routing and delivery of addressed frames.
- **Re-association**: Enables an established association to be transferred from one access point to another, allowing a mobile station to move from one BSS to another.
- **Disassociation**: A notification from either a station or an access point that an existing association is terminated.
- **Authentication**: Used to establish the identity of stations to each other. The standard does not mandate any particular authentication scheme, which could range from insecure handshaking to public-key encryption schemes.
- **Privacy**: Used to prevent the contents of message from being read by other than the intended recipient. The standard provides for the optional use of encryption to assure privacy.

1.3 Attributes of Wireless LAN's

Wireless LANs must adhere to the many of the same rules as traditional wired LANs, including full connectivity to stations, the ability to broadcast, high capacity, etc. In addition, wireless LANs have some special requirements unique to their forms of communication. A few of these follow:

- **Throughput** - Due to the decreased bandwidth of radio and IR channels, the Medium Access Control (MAC) protocol should make as efficient use of this available bandwidth as possible.
- **Backbone Connectivity** - In most cases, wireless LANs connect to some sort of internal (wired) network. Therefore, facilities must be provided to make this connection. This is usually one station that serves as the Access Point (AP) to the wired LAN for all stations.
- **Power Considerations -** Often times, wireless stations are small battery powered units. Algorithms that require the station to constantly check the medium or perform other tasks frequently may be inappropriate.
- **Roaming -** Wireless stations should be able to move freely about their service area.
- **Dynamic** - The addition, deletion, or relocation of wireless stations should not affect other users.
- **Licensing** - In order to gain widespread popularity, it is preferred that FCC licenses not be required to operate wireless LAN's.

1.4 Wi-Fi Configuration

IEEE 802.11b LANs can be deployed in either *ad hoc* configuration or *infrastructure* configuration.

The ad hoc configuration refers to the peer-to-peer setup, where a bunch of devices with 802.11b network interface cards (NICs) can establish a network and communicate with each other without any infrastructure support. The connectivity of the nodes in this network is limited to their peers.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

On the other hand, the infrastructure or the access-point setup uses a central access-point (base-station) to form a network. The access-point is usually connected to a wired network as a bridge for next hop connectivity. Every packet transmitted by a wireless node is destined for the access-point, which takes care of further routing/switching. Most of the corporate and large-scale wireless networks are setup in the infrastructure mode of operation.

There are two different classes of infrastructure operation. These are *basic service set* (BSS) and *extended services set* (ESS). In BSS configuration each wireless node is *associated* with an access-point and this association remains unchanged indefinitely, whereas, in ESS a mobile node can roam around and *disassociate* from current access-point and associate with a new access-point or *re-associate* with the previous access-points. The ESS is basically meant to provide roaming support.

IEEE 802.11b technology has achieved a high level of penetration in the wireless networking arena. It is being regarded as the *de facto* wireless standard for wireless LANs.

1.5 Access point varieties

The typical Wi-Fi setup contains one or more Access Points (APs) and one or more clients. An AP broadcasts its SSID (Service Set Identifier) via packets that are called beacons, which are broadcasted every 100 ms. The beacons are transmitted at 1 Mbit/s, and are relatively short and therefore are not of influence on performance. Since 1 Mbit/s is the lowest rate of Wi-Fi, it assures that the client, who receives the beacon, can communicate at the rate of at least 1 Mbit/s. Based on the settings (e.g., the SSID), the client may decide whether to connect to an AP or not. Also the firmware running on the client Wi-Fi card is of influence. For example, for two AP's of the same SSID that are in range of the client, the firmware may decide based on signal strength to which of the two AP's it will connect. The Wi-Fi standard leaves connection criteria and roaming totally open to the client. This is the strength of Wi-Fi, but also means that one wireless adapter may perform substantially better than the other adapter. Since Windows XP™ there is a feature called *zero configurations*, which makes the user show any network available and let the end user connect to it on the fly. In the future, wireless cards will be more and more controlled by the operating system. Microsoft's newest feature called *SoftMAC* will take over from on-board firmware. Having said this, roaming criteria will be totally controlled by the operating system. Wi-Fi transmits in the air; it has the same properties as non-switched Ethernet network. Even collisions can therefore appear like in non-switched Ethernet LAN's.

An 802.11b wireless network adapter can operate in two modes, Ad-Hoc and Infrastructure. In infrastructure mode, all the traffic passes through a wireless 'access point'. In Ad-hoc mode all the computers talk directly to each other and do not need an access point at all.

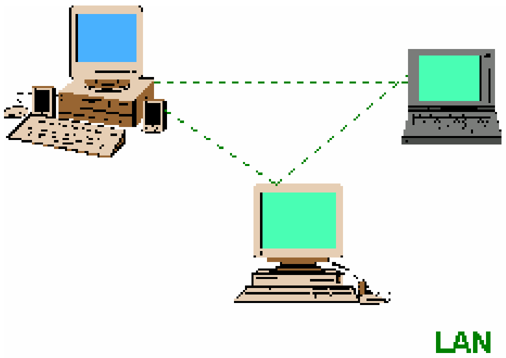


Figure 1: 802.11b without an Access Point.

1.5.1 Simple 802.11b wireless Ethernet network without an access point

Two or more wireless Ethernet computer (802.11b) may communicate with each other without a wireless access point (see Fig. 1). The wireless cards must be set to 'AdHoc' mode instead of 'infrastructure' mode.

1.5.2 Simple 802.11b wireless Ethernet network with an access point

Wireless Ethernet adapter defaults to 'infrastructure' mode, a communication method that requires a wireless access point (see Fig. 2). An access point controls encryption on your network and may bridge or route your wireless traffic to a wired Ethernet network (or the Internet). Access points that act as routers can also assign IP addresses to your PC's using DHCP services.

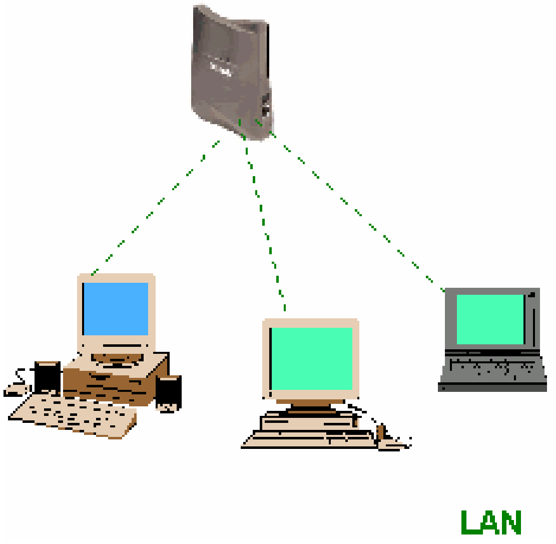


Figure 2: 802.11b with an Access Point.

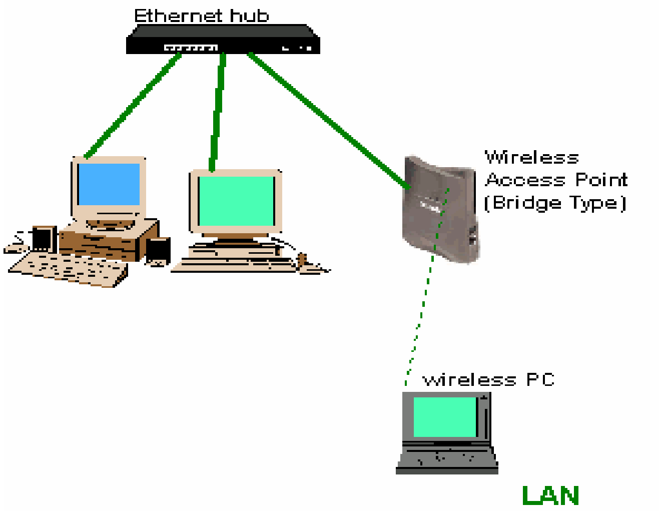


Figure 3: 802.11b with a Wired Ethernet Network.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

1.5.3 Bridging a wireless 802.11b network with a wired Ethernet network

The wireless access point in this diagram (Fig. 3) acts as a network bridge. Because of the bridge, the wireless PC appears to be on the same network as the traditional Ethernet PC's. They may communicate back and forth with each other freely.

1.5.4 Bridging a wireless 802.11b network with a wired Ethernet network using Windows XP™

The computer running Windows XP™ in the middle diagram (Fig. 4) acts as a network bridge. It has both a wired Ethernet adapter and an 802.11b wireless adapter. Windows XP™ was set up using the Media Bridge services. Because of the bridge, the wireless PC appears to be on the same network as the traditional Ethernet PC's. They may communicate back and forth with each other freely.

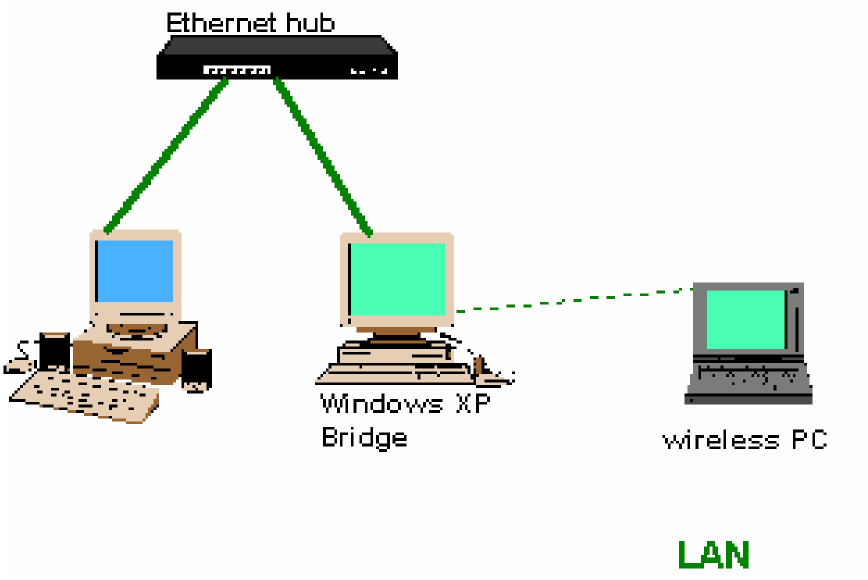


Figure 4: Bridging a Wireless 802.11b Network.

2. IEEE 802.11b MAC overview

IEEE 802.11b is the standard for Medium Access Control (MAC) and Physical Layer (PHY) specifications for wireless LANs. The PHY specifications deal with modulation techniques, error correcting codes, radio characteristics, physical layer convergence, and other signaling related issues.

IEEE 802.11b MAC protocol is based on the CSMA/CA protocol [3], which uses physical carrier sense, as well as virtual carrier sense to avoid collisions and packet loss. Physical carrier sense is used to avoid collisions at the sender, whereas, virtual carrier sense is used to avoid collisions at the receiver and address the *hidden node* problem present in wireless networks. The virtual carrier sense uses regular Request-To-Send (RTS) and Clear-To-Send (CTS) channel reservation mechanism. 802.11b MAC improves the link layer reliability by including explicit ACKs for each data frame.

Upon failure to receive an ACK, the data frame is repeatedly retransmitted till an ACK is received. The maximum number of retransmissions is a configurable parameter for each individual node and is usually set to seven. Thus each successful transmission follows the so-called *4-way handshake* protocol of RTS-CTS-DATA-ACK. A node may choose to disable the virtual carrier sense to reduce its overhead when the probability of existence of hidden nodes is known to be small.

802.11b MAC includes two coordination functions for channel access, namely, Distributed Coordination Function (DCF) and Point Coordination Function (PCF). The DCF specifies channel contention mechanism for normal mode of operation, whereas, PCF specifies a mechanism for channel access in a contention free fashion. PCF requires the presence of a *point coordinator* (PC) and can be used only in infrastructure mode of operation.

2.1 Distributed Coordination Function

In the normal mode of operation, the IEEE 802.11b MAC uses a Distributed Coordination Function (DCF) for media access. DCF is an implementation of CSMA/CA protocol, which follows the 4-way handshaking protocol for data transmissions. In DCF, whenever a node is ready to transmit data, it senses the channel to be idle for a period of Distributed Inter Frame Spacing (DIFS).

Following this, it generates a random back-off timer. After the back-off timer expires, the node sends a short Request-To-Send (RTS) message to the intended receiver of data. If this message is received properly by the receiver and if it is able to receive any transmission, it responds back with a short Clear-To-Send (CTS) message.

A node may not be able to receive any transmission if some other node in its vicinity has already reserved the channel for packet reception or transmission. Both RTS and CTS messages carry the duration information for which the channel is going to be occupied by the proposed data transmission.

Upon hearing RTS and CTS, all other nodes in the vicinity of the sender and receiver update their Network Allocation Vectors (NAVs) with the information about the duration for which the channel is going to be busy. NAV is essentially a channel reservation vector.

Thus, all nodes in the vicinity of the sender and receiver defer their transmissions and receptions to avoid collisions. The CTS message is followed by the DATA transmission, which is acknowledged by the receiver by sending an ACK message if the DATA is received successfully. The data is repeatedly retransmitted in the absence of ACKs till a threshold number of retransmissions are carried out. Once the retransmissions exceed the threshold, the transmission is assumed to be unsuccessful.

A timeline for DCF message exchanges is shown in Fig. 5. The sense period of DIFS is larger than SIFS. This ensures that no new transmission attempts interfere with the ongoing transmission.

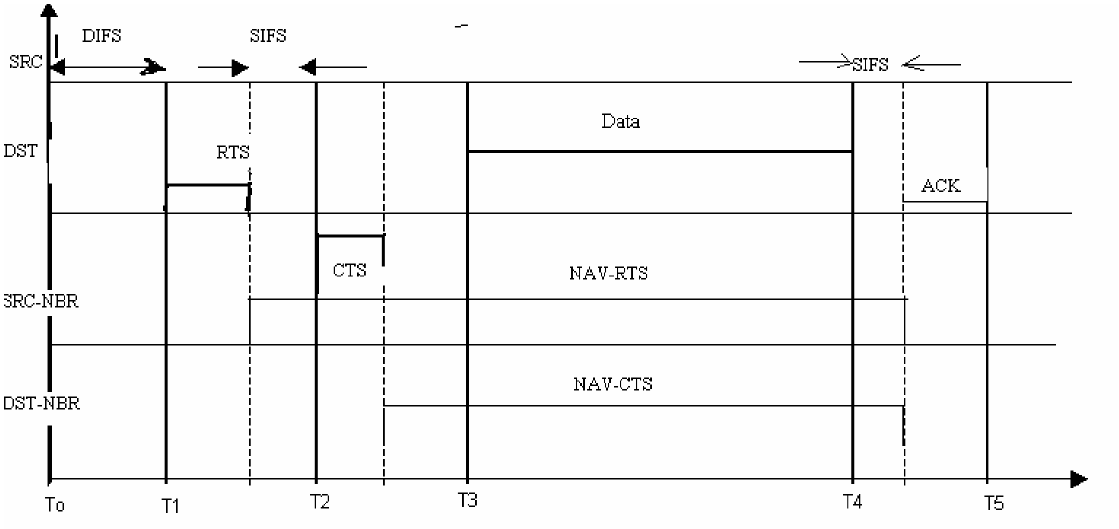


Figure 5: Message exchanges for DCF. Each DATA packet is preceded by RTS and CTS messages.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

DCF provides a mechanism for collision avoidance by performing a virtual carrier sense through RTSCTS message exchanges. This is necessary to solve the *hidden node problem*. However, a node may chose to resort to a 2-way handshaking mechanism where data packets are transmitted without RTS-CTS message exchanges. The receiver acknowledges the packet back by responding with an ACK message. This mechanism can be used for small packets where the overhead of RTS/CTS message exchange can be traded off for small probability of collisions.

2.2 Point Coordination Function

IEEE 802.11b standard provides a very rudimentary support for Quality of Service in its infrastructure mode of operation. The MAC layer in terms of Point Coordinated Function (PCF) provides this support.

PCF is a MAC coordination facility that may exist on access-points to differentiate between the traffic flows from different nodes. PCF is an optional capability for access points and its implementation is not mandatory. Very few commercially available access-points for 802.11b networks actually provide this facility. Moreover, there are no clear mechanisms for individual nodes to participate in PCF and exploit the quality of service mechanism provided by it.

The access-point of a cell acts as a coordinator called the *point coordinator* (PC) for that cell. All nodes in 802.11b network obey the medium access rules of the PCF, since these are based on DCF, which is followed by all nodes.

In infrastructure mode of 802.11b, the time period is divided into periodic **superframe***s,* which start with the so-called **beacon frames.** A beacon frame in 802.11b is a management frame sent by an access point to carry out time synchronization and deliver protocol related information to all nodes. Regardless of PCF functionality, the access point periodically sends beacon frames. Each superframe is divided into two units, namely, *Contention Free Period* (CFP) and *Contention Period* (CP). CFP is the period when contention free channel access is provided by the PC to individual nodes. CP is the period when all nodes contend for the channel using DCF.

If the PCF functionality is not provided by the access point, then entire superframe is the contention period. The PC determines the extent of division of a superframe into CFP and CP, which can be arbitrary, but it is mandatory to have a CP of a minimum duration that allows at least one node to transmit one frame under DCF.

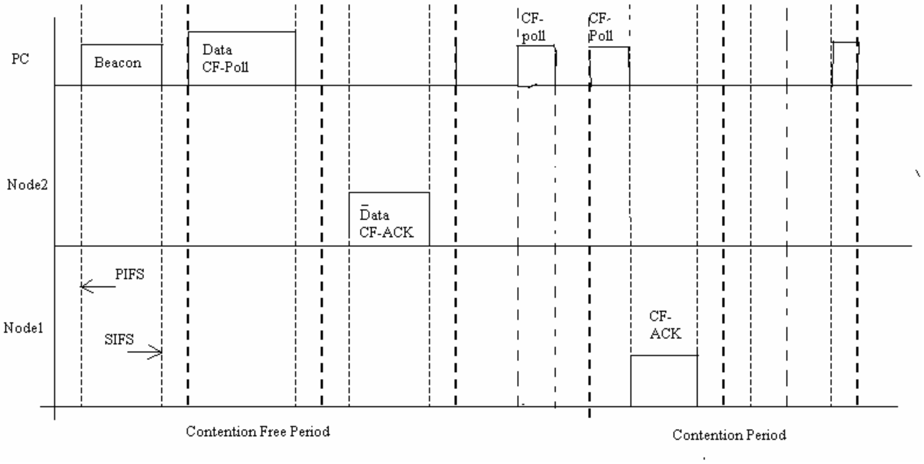


Figure6: A PCF Superframe Construction. Each Superframe is divided into Contention-Free and Contention Periods.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

Figure 6 shows the activity of a wireless network during a superframe. At the beginning of superframe the PC waits for a period PCF Inter Frame Space (PIFS) and then transmits the beacon frame. If the PC supports PCF and the list of nodes that are interested in being polled is not empty, the PC sends a CF-Poll (or DATA+CF-Poll) frame to one of the nodes after waiting for channel to be idle for SIFS. In response, the node can respond with a DATA + CF-ACK or just CF-ACK if no data is ready to be sent. The response is sent after sensing the channel to be idle for an SIFS period. If there is no response to CF-Poll frame, the PC sends CP-Poll to next node after waiting for an idle period of PIFS. At the end of CFP, the PC sends a CF-END frame to begin the contention period using DCF.

Thus in CFP, each polled node transmits frames in a contention free manner. In CFP, RTS/CTS handshaking is not carried out. During the entire CFP the PC is in control because it accesses channel after sensing the channel to be idle for PIFS duration. PIFS is much smaller than DIFS, which is the period for which every node in DCF should sense the channel to be idle. The shorter duration of PIFS compared to DIFS ensures that no node can contend for the channel except either the PC or the node that has been recently polled.

3 Security

Security has been a long trade off with Wi-Fi. Early wireless networks heavily leaned on VPNs to provide Layer 3 security, which – aside from the additional overhead of encapsulation and challenges of roaming, Quality of Service, client support and scalability – left the IP network vulnerable to attacks.

3.1 WEP-Wired Equivalent Privacy

The first security measures introduced for Wi-Fi was WEP. Wired Equivalent Privacy (WEP) is a scheme to secure Wi-Fi. Because a wireless network broadcasts messages using radio, it is particularly susceptible to eaves-dropping. WEP was intended to provide comparable confidentiality to a traditional wired network.

WEP is part of the IEEE 802.11 standard ratified in September1999. WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Standard 64-bit WEP uses a 40-bit key, to which a 24-bit initialization vector (IV) is concatenated to form the RC4 traffic key. WEP was susceptible to attacks and poorly implemented by vendors. Several serious weaknesses were identified, and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004.

3.2 WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access (WPA), an improved security standard for wireless networks, is the first generation of advanced wireless security, providing enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. WPA is based on a sub-set of the IEEE Institute of Electrical and Electronics Engineers.

WPA is a powerful, standards-based, interoperable security technology for Wi-Fi networks. It provides strong data protection by using encryption as well as strong access controls and user authentication. WPA can be enabled in two versions - WPA-Personal and WPA-Enterprise.

WPA-Personal protects unauthorized network access by utilizing a set-up password. This is normally suitable for small offices or home computers.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

WPA-Enterprise is for any large corporation, business or organization. The enterprise market can verify network users through a server. WPA utilizes 128-bit encryption keys and dynamic session keys to ensure your wireless network's privacy and enterprise security.

WPA is designed for use with an 802.1X authentication server, which distributes different keys to each user. However, it can also be used in a less secure "pre-shared key" (PSK) mode, where every user is given the same pass-phrase. The Wi-Fi Alliance® calls the pre-shared key version *WPA-Personal* or *WPA2-Personal* and the 802.1X authentication version *WPA-Enterprise* or *WPA2-Enterprise*.

Data is encrypted using the RC4 stream cipher, with a 128-bit key and a 48-bit initialization vector (IV). One major improvement in WPA over WEP is the Temporal Key Integrity Protocol (TKIP), which dynamically changes keys as the system is used. When combined with the much larger IV, this defeat the well-known key recovery attacks on WEP.

In addition to authentication and encryption, WPA also provides vastly improved payload integrity. The cyclic redundancy checks (CRC) used in WEP is inherently insecure; it is possible to alter the payload and update the message CRC without knowing the WEP key. A more secure message authentication code (usually known as a MAC, but here termed a *MIC* for "Message Integrity Code") is used in WPA, an algorithm named "*Michael*". The MIC used in WPA includes a frame counter, which prevents replay attacks being executed; this was another weakness in WEP.

WPA was formulated as an intermediate step towards improved the 802.11 security for two reasons: first, 802.11i's work. By increasing the size of the keys and IVs, reducing the number of packets sent with related keys, and adding a secure message verification system, WPA makes breaking into a Wireless LAN far more difficult. However, it is subject to a packet forgery attack. To limit this risk, WPA networks shut down for 60 seconds whenever an attempted attack is detected.

3.3 WPA2

WPA2 is the certified form of IEEE 802.11i tested by the Wi-Fi Alliance. WPA2 implements the mandatory elements of 802.11i. In particular, the MIC ("Michael") algorithm is replaced by a message authentication code, CCMP, that is considered fully secure, and RC4 is replaced by AES (Advanced Encryption Standard). Official support for WPA2 in Microsoft Windows XP™ was included.

Both WPA and WPA2 include two authentication modes: personal and enterprise (see Table 1). WPA2–personal generates a 256 bit key from plain text pass phrase sometimes called Pre-shared key mode (PSK, also known as *personal* mode), is designed for home and small office networks that cannot afford the cost and complexity of an 802.1X authentication server.

Table 1: Wireless Protocols Compared

Description	WEP	WPA	WPA2
Authentication	N/A	IEEE 802.1x/EAP/PSK	IEEE 802.1x/EAP/PSK
Cryptographic Algorithm	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Per-frame keying	No	Yes	Yes
Initialization Vector length	24 bits	48bits	48bits

The PSK (as well as Service Set Identifier and SSID length) from the mathematical basis for the PMK (Pairwise Master Key) that's used to initiate a four way handshake and generate the PTK (Pairwise Transient Key) or session key between the wireless user device and access point. WPA2

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

personal poses challenges in key distribution and maintenance, making it fit for small offices but not for enterprise.

WPA2-Enterprise addresses concerns regarding distributing and managing static keys, and controls access on a per account basis by trying in to most organizations' authentication services. This mode requires credentials, such as a username and password, a certificate or one time password, and authentication occurs between the station and central authentication server. WPA2 gives wireless networks both confidentiality and data integrity.

4. Laboratory Exercise

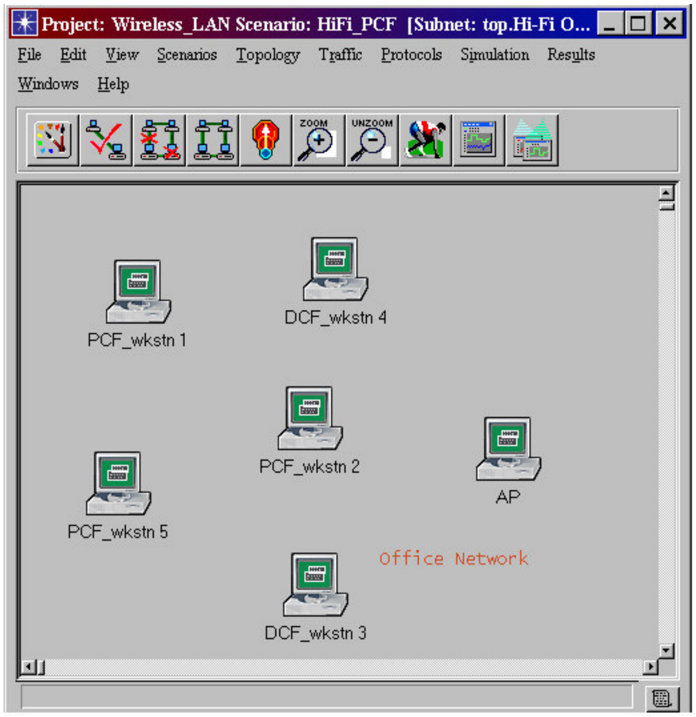
4.1 Objective

The objective of this laboratory exercise is to study the number of retransmissions for a PCF enabled station over non-PCF enabled station.

4.2 Scenario

The scenario has five Wi-Fi-based workstations in a simple network configuration (Infrastructure BSS), which demonstrates the PCF access method used by Wi-Fi. PCF provides contention free (CF) frame transfer. The Traffic flows between the stations have been configured as:

PCF1 ----------> PCF2
DCF3 ---------> DCF4
PCF5 ---------> PCF1.

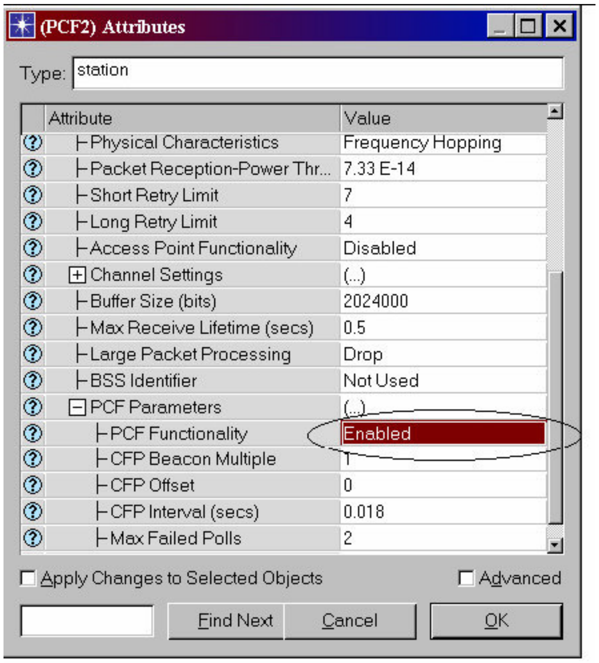


Project: Wireless_LAN Scenario: HiFi_PCF [Subnet: top.Hi-Fi O...

Figure 7: Network of the Wi-Fi Laboratory Exercise.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

All the PCF related configuration parameters are grouped into a single compound attribute "PCF parameters. The attributes for PCF and DCF workstations are shown in Fig. 8.



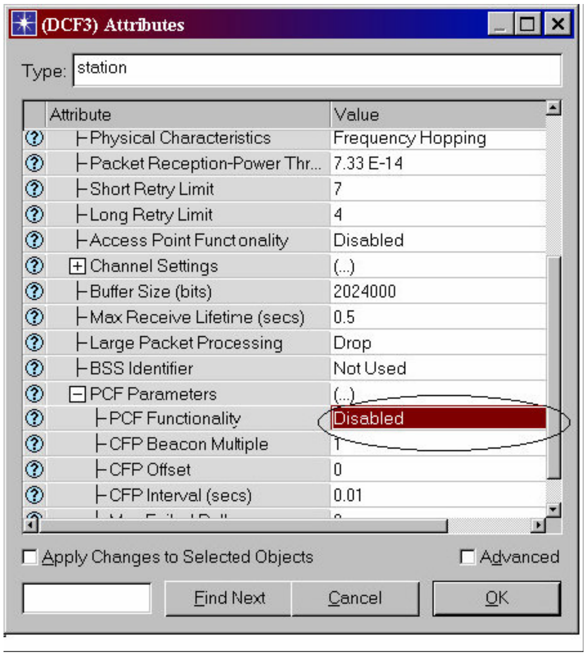
(PCF2) Attributes

Type: station

Attribute	Value
Physical Characteristics	Frequency Hopping
Packet Reception-Power Thr...	7.33 E-14
Short Retry Limit	7
Long Retry Limit	4
Access Point Functionality	Disabled
⊞ Channel Settings	(...)
Buffer Size (bits)	2024000
Max Receive Lifetime (secs)	0.5
Large Packet Processing	Drop
BSS Identifier	Not Used
⊟ PCF Parameters	(...)
PCF Functionality	Enabled
CFP Beacon Multiple	1
CFP Offset	0
CFP Interval (secs)	0.018
Max Failed Polls	2

□ Apply Changes to Selected Objects □ Advanced

Figure 8: The Attributes for PCF Workstations.



(DCF3) Attributes

Type: station

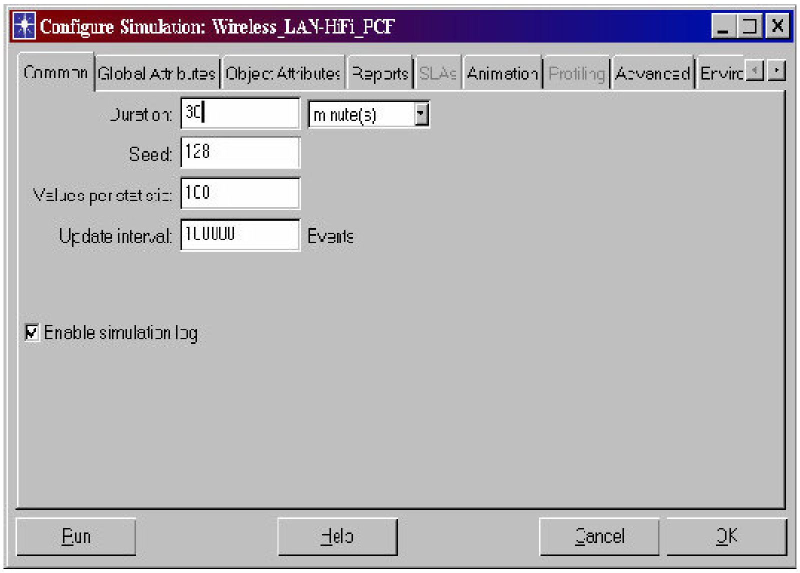
Attribute	Value
Physical Characteristics	Frequency Hopping
Packet Reception-Power Thr...	7.33 E-14
Short Retry Limit	7
Long Retry Limit	4
Access Point Functonality	Disabled
⊞ Channel Settings	(...)
Buffer Size (bits)	2024000
Max Receive Lifetime (secs)	0.5
Large Packet Processing	Drop
BSS Identifier	Not Used
⊟ PCF Parameters	(...)
PCF Functionality	Disabled
CFP Beacon Multiple	1
CFP Offset	0
CFP Interval (secs)	0.01

□ Apply Changes to Selected Objects □ Advanced

Figure 9: The Attributes for DCF Workstations.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

After setting the parameters of all the workstations, the run configuration for simulations can be set as shown in Fig. 10.



Duration: 30 minute(s)
Seed: 128
Values per statistic: 100
Update interval: 100000 Events

☑ Enable simulation log

Figure 10: The Configuration Simulation Window.

The objective is to study the number of retransmissions for a PCF enabled station over non-PCF enabled station. After executing the simulation, following graphs (Figs. 11 and 12) are generated.

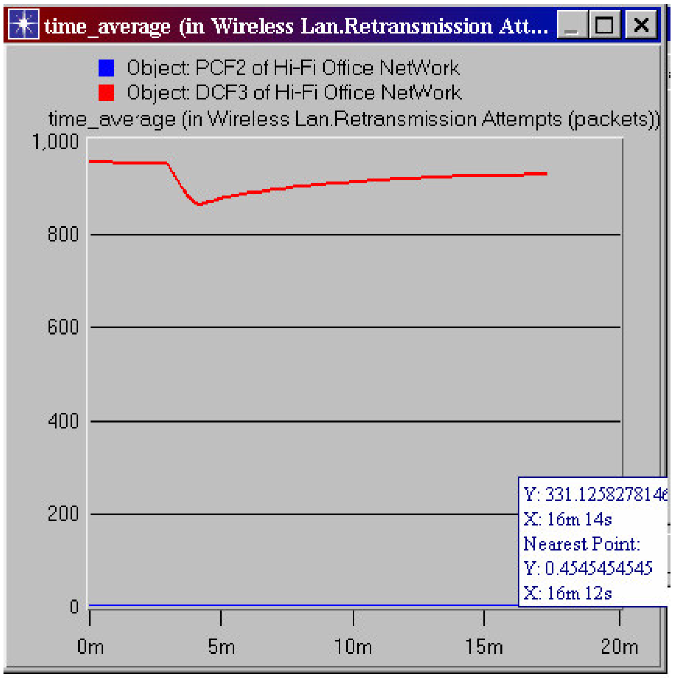


Figure 11: Number of Retransmission Attempts.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

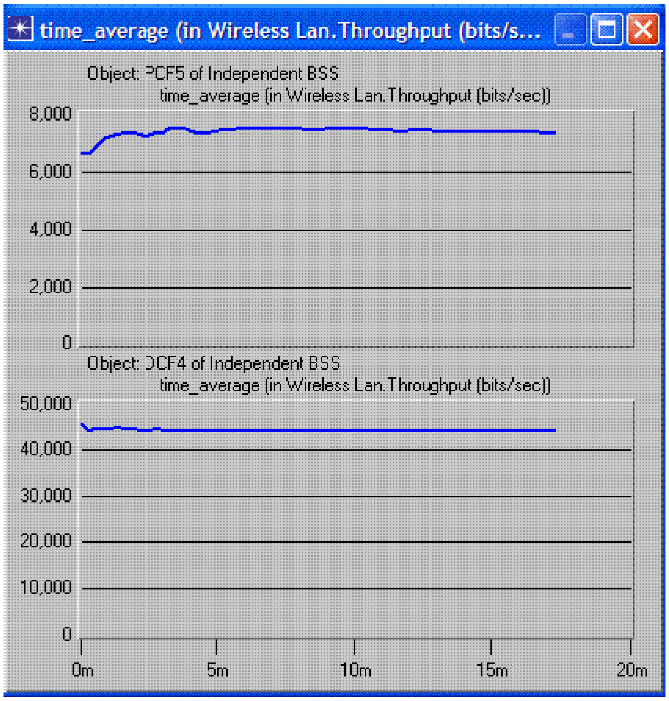


Figure 12: Throughput for PCF and DCF Workstations.

The overlaid view is shown in Fig. 13.

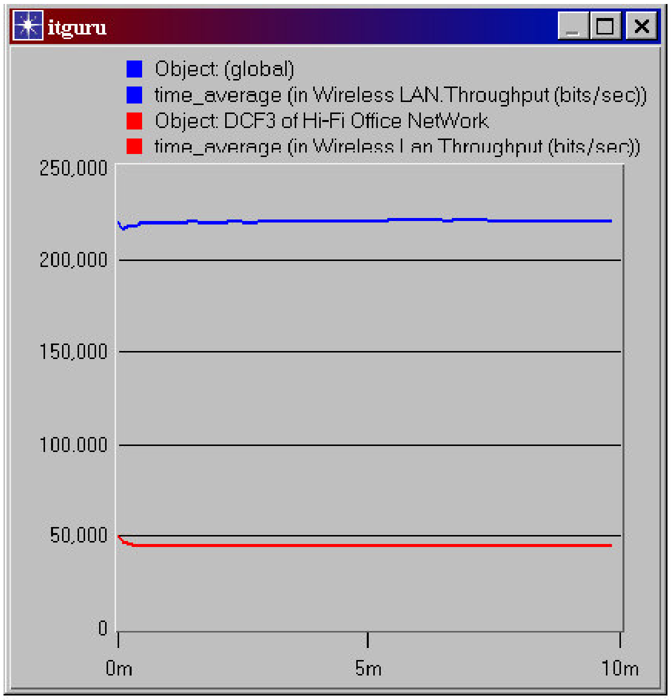


Figure 13: Throughput for Wireless LAN and DCF Workstations.

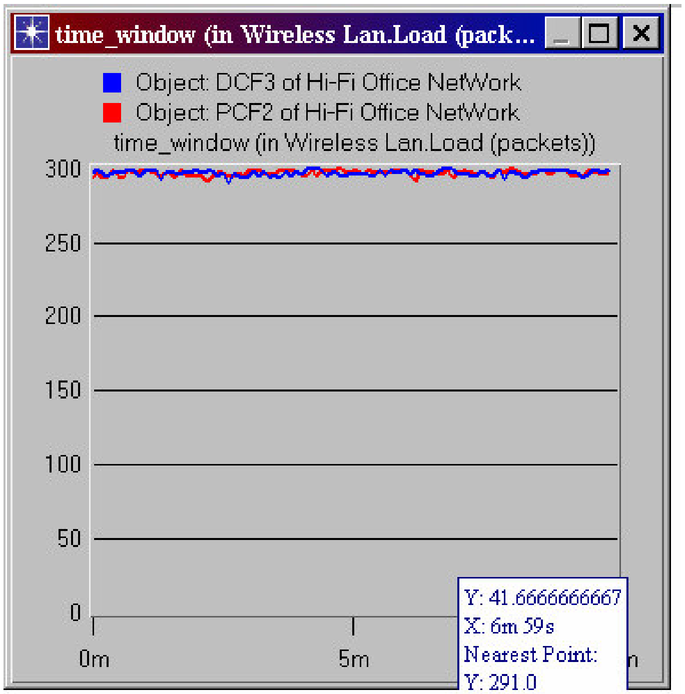


Figure 14: Load in Packets for both workstations.

The load (measured in packets) for PCF and DCF stations is shown in Fig. 14.

4.3 Discussion of the Results

The number of retransmissions for a PCF enabled node is significantly less compared to the non-PCF node load. Also, the throughput is higher for a PCF enabled compared to the non-PCF workstation with a similar load. PCF enabled station can transmit data during both the Contention-Free period (CFP) and Contention period (CP).

5. Conclusion

In this paper, the concept of the Wi-Fi technology and important factors of Wi-Fi have been explained. The IEEE 802.11b standard is the most dominant wireless LAN technology nowadays. Wi-Fi products are widely available in the market. Different brands of access points and client network interfaces are interoperable at a basic level of service. Wi-Fi networks support roaming, in which a mobile client station, such as a laptop computer, can move from one access point to another, as the user moves around a building or area. Wi-Fi is a global set of standards. Unlike cellular carriers, the same Wi-Fi client works in different countries around the world.

Wi-Fi is compatible with some gaming consoles and handheld, allowing online play at any access point. Commercial Wi-Fi services are available in places such as Internet cafes, called as "*Hot-spots*", coffee houses, and airports around the world.

Some serious disadvantages are yet to overcome though. Wi-Fi networks have limited range. Interference of a closed or encrypted access point with other open access points on the same or a neighboring channel can prevent access to the open access points by others in the area. This can pose a

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

problem in high-density areas, such as large apartment buildings, where many residents are operating Wi-Fi access points. Access points could be used to access personal information transmitted from Wi-Fi users. Interoperability issues between brands or deviations in the standard can cause limited connection or lower throughput speeds. Technology is rapidly evolving in this area. All these problems are the major area of research. Hopefully, these problems will be able overcome in near future.

References

[1] Janice Reynolds. *Going Wi-Fi: A Practical Guide to Planning and Building an 802.11 Network*. CMP, 2003.

[2] Frank Bulk. ABC's of WAP2 Wi-Fi Security. *Network Computing Magazine*. Retrieved October 23, 2006, from http://magazine-directory.com/Network-Computing.htm

[3] Tom Sheldon. *Encyclopedia of Networking*, New York: McGraw-Hill, 2001.

[4] Frank Ohrtman and Konrad Roeder. *Wi-Fi Handbook*. New York: McGraw-Hill, 2003.

[5] Wi-Fi. Retrieved October 23, 2006, from http://en.wikipedia.org/wiki/Wi-Fi

[6] Wireless Fidelity. Retrieved October 23, 2006, from http://www.wi-fi.org

Glossary

ACK: Acknowledgment.

Ad-Hoc Mode: A client setting that provides independent peer-to-peer connectivity in a wireless LAN. Also see Infrastructure Mode.

BPS: Bits Per Second.

BSS: Basic Service Set. A bunch of machines forming a cell.

CSMA/CA: Carrier Sense Multiple Access/Collision Avoidance. CSMA/CA is the medium access method used by IEEE 802.11 WLANs.

DSSS: Direct-sequence spread-spectrum. One of two types of spread-spectrum radio technology used in wireless LAN (WLAN) transmissions. To increase a data signal's resistance to interference, the signal at the sending station is combined with a higher-rate bit sequence that spreads the user data in frequency by a factor equal to the spreading ratio.

DIFS: Distributed Inter Frame Spacing

DCF: Distributed Coordination Function

ESS: Extended Service Set. Using Wi-Fi beyond a BSS, gluing together several BSS

FHSS: frequency hopping spread spectrum. A modulation technique, which spreads data across the entire transmission spectrum by transmitting successive data on different channels ("hopping").

HomeRF: Home Radio Frequency. It is a short-range wireless technology that uses the license-free frequency band 2.4 GHz. HomeRF supports both wireless audio and data, as it is a combination of Wireless LAN and DECT.

IEEE: Institute of Electrical and Electronics Engineers.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).

Infrastructure Mode: A client setting providing connectivity to an Access Point (AP). As compared to Ad-Hoc Mode, where PCs communicate directly with each other, clients set in Infrastructure Mode all pass data through a central AP.

LAN: Local Area Network, A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves.

MAC: Medium Access Control. In a WLAN network card, the MAC is radio controller protocol.

NAV: Network Access Vector: A time slot reservation, in microseconds.

RTS/CTS: Request To Send, Clear To Send. Reservation mechanism.

SSID: Service Set Identifier. A character-string identifier for an ESS.

TCP/IP: Transmission Control Protocol / Internet Protocol.

WEP: Wired Equivalent Privacy. WEP is a scheme to secure Wi-Fi. Because a wireless network broadcasts messages using radio, it is particularly susceptible to eavesdropping.

Wi-Fi: Wireless Fidelity, a wireless technology association.

WPA: Wi-Fi Protected Access. WPA is an improved security standard for wireless networks

* **VANDANA WEKHANDE** has come to the U.S. from Maharashtra, India. She received her B.Eng. in Computer Science in 1993 and worked as a Software Developer for Autel, Inc. in Mumbai, India, for 3 years. After that she worked as an Assistant Lecturer for the Engineering College in Mumbai for 2 years. After coming to the United States in 2001, she worked as a private consultant for 2 years. Nowadays she is a full-time student pursuing a M.S. degree in Computer Science at Rivier College.

ISSN 1559-9388 (online version), ISSN 1559-9396 (CD-ROM version).