System Communication based on Wi-Fi Technology using 802.11x

N. P. Giradkar
Professor
SRPCE,Nagpur

C. D. Raut
Research Scholar
SRPCE,Nagpur

ABSTRACT
Wi-Fi Think of it as an eighteenth wheeler screaming down the pike, carrying the future of computing with it. The driver is friendly. anyone can stick out their thumb and hitch a ride, or be left in the dust. WIFI, in the broadest sense is a term used for a specific protocol to network host computer to another computer or network. It allows to connect to the Internet even with a couch at home, a bed in a hotel room or a conference room at work without wires with a speed several times faster than the fastest cable connection. This paper proposed to attempt a review on all the major aspects of wireless networking and the 802.11x protocol corresponding to Wi-Fi .The paper deals with the basic concepts of wireless networking and goes into the in-depth of 802.11x protocol which forms the backbone of the upcoming technology, Wi-Fi. Seamless networking is neither a compromise anymore nor a showpiece of high end business markets. The wave of the future is already sweeping through.

1. INTRODUCTION
Over the past decade, two trends have been clearly identifiable in the area of personal computing; first, computers have gotten smaller and much more portable. Secondly, the internet has increasingly become a bigger part of the daily routines of many people, especially college students. The combination of these two trends have paved the way for the introduction of a fast and reliable wireless networking infrastructure so that people can use their portable computers without being restrained by cables. Wireless local-area networks (WLAN) are evolving towards the development of broadband applications, including multimedia services in a way to compete with wired LAN systems. It is expected that rapid growth of mobile users will eventually demand the development of new applications with broadband access and bit rates higher than 54 Mbps, what is currently offered by IEEE 802.1 la and g standards. Only 50-60% of that nominal bit rate is devoted to user traffic, due to the overhead imposed by physical-layer (PHY) frame header, preamble transmission and requirement that each sent frame must be acknowledged. Therefore, the aim of today's research effort is to provide high bandwidth WLAN communication system with similar performance, reliability and security compared to its wired counterpart. As WLAN technology matures, newer features and functionality will continue to be made available. Standardization organizations, like IEEE are providing continuous effort to meet new demands from users by introducing new standards as well as minimizing shortcomings of the previous standards [1, 7].

What is Wi-Fi ?

Wi-Fi is just one aspect of wireless networking used in computing today. It's powerful. Wi-Fi networks use radio technologies called IEEE 802.11b or 802.11a to provide secure, reliable, fast wireless connectivity. A Wi-Fi network can be used to connect computers to each other, to the Internet, and to wired networks (which use IEEE 802.3 or Ethernet). Wi-Fi networks operate in the unlicensed 2.4 and 5 GHz radio bands, with an 11 Mbps (802.11b) or 54 Mbps (802.11a) data rate or with products that contain both bands (dual band), so they can provide real-world performance similar to the basic 10BaseT wired Ethernet networks used in many offices. Wi-Fi on the other hand is a term used for a specific protocol to network your computer to another computer or network. The industry term for Wi-Fi is 802.11b and it is also known as "Airport", an Apple branded name for the technology. There are two main components to a Wi-Fi network. First, you will need an "access point" (called the "base station" with Apple's Airport technology). Second, we will need a network card installed in your computer. Access points generally run in the $200 price range while the network cards will cost you about $100. Once you have the access point configured and the network card installed, you can transmit data from your computer to the base station up to 150 feet away at 10 MBps with no cables.

2. BASICS OF WIRELESS NETWORKING AND WI-FI
The first wireless LAN was created in at the University of Hawaii in 1971.Researches at the university combined radio technology with network technology to create a bi-directional star network that connected seven workstations over four islands. ALOHANET, as it was called, made no use of phone lines or satellites. Since then, wireless technology has made its way into homes, classrooms, coffee houses, restaurants, airports, city parks and college campuses. In 1997, the Institute of Electrical and Electronic Engineers (IEEE) drafted the 802.11 standard for wireless local area networking. In 1999, networking hardware companies accepted the standard and began manufacturing products using the 802.11b protocol which operated in the 2.4 GHz range and was capable of transmitting at speeds of 11 megabits per second. The 802.11a protocol was also released in 1999, operating at 5.8 GHz with transmissions speeds of 54 megabits per second, but its cost was prohibitively high. Most components in homes and offices today are based on the 802.11b protocol, due to its solid transmission speeds and reasonable price. In general, there are three types of wireless

a **Fig.1 Pure wireless network**

Fig.2 Mixed environment network

components available in the consumer or small business market today. First, there are wireless network adapters. These adapters

re available in PCMCIA, PCI, USB, and even Compact Flash. Installation of one of these adapters into a host allows that host to communicate with other machines equipped with wireless network adapters, or with wireless access points. Wireless access points are small base stations that have a wired connection to some sort of supporting network infrastructure. An access point will provide connectivity to the wired network and to other wireless hosts for all of the wireless hosts within its range. Most access points available in the market today have a number of more advanced features, such as the ability to dynamically assign IP addresses to their wireless clients, the ability to perform network address translation (i.e. function as a router), traffic encryption capability, and packet filtering abilities. Additionally, many access points available for home use have an additional wired Ethernet hub or switch built in, such that they may be used in conjunction with a pre-existing wired network. Finally, wireless bridges will connect a wired network directly to a wireless network. A bridge, in general, will connect one network to another by selectively forwarding data across itself if the bridge determines that the data is destined for the network on its other side. In the wireless world, it is often helpful to think of a wireless bridge as a "wireless extension cord" that, when attached to a wired Ethernet device, would have the same effect as connecting the wired device directly to a port on an access point. Wireless devices can be connected in two basic topologies. First, they can be connected in a star topology, which involves all of the wireless hosts communicating with a central host, or access point, and never to each other. This is the most common wireless network topology. Wireless hosts can also communicate directly with each other, without the use of an access point, as long as they are within range of one another. This topology, known as mesh topology or ad-hoc networking, is less common, but sometimes much more convenient than star topology since it requires no more hardware than the hosts themselves. A home or office network made out of these components typically will use some variant of the star topology. In a purely wireless home or office network, all of the hosts will have wireless network adapters installed, and will only communicate with the central access point. The access point has a direct connection to a wired network, and in The case of a home or small business, this wired network is simply the internet. Most home or small business networks will either have a pre-existing wired network in place or have some components which, for one reason or another, cannot accommodate a wireless adapter. In this case, a mixed network topology is necessary network adapter. It should also be noted that the

wireless router in must be a model that contains a wired Ethernet hub or switch of some kind. Finally, in a variant of the Mixed Environment network, a component or an entire network that cannot support a wireless adapter might be in a physical location that is difficult or impossible to reach using a wired network. In this case, the PlayStation 2 is such a device. To reach it, a wireless bridge can reach the access point and supply access to the rest of the network and to the Internet. Clearly, one of the biggest problems associated with a wireless network is that of security. With a medium of air, any wireless traffic can easily be intercepted by any number of malicious entities. With wired networking, this wasn't a concern because a third party would have to have physical access to a network in order to intercept
traffic. robin order to combat this problem, 802.11b includes the wired equivalency protocol (WEP). WEP has two main theoretical functions. First, it disallows unauthorized access to the wireless network. That is, a wireless host would have to have the WEP password in order to become a member of the wireless network. Secondly, it encrypts all packets so that they cannot be read if they are intercepted. Unfortunately, WEP doesn't employ a very strong encryption algorithm, and it can be broken by anyone who has the time and the means to intercept a great deal of data from the network. There are other ways to protect traffic from prying eyes of hackers. Changing administrative passwords, disabling DHCP, disabling network advertisement, and enabling MAC address filtering are all ways of making a given wireless network hidden from view. In large or dynamic networks (such as public hot spots) these can make use of the network extremely difficult, if not completely impossible. Thus, there are a few other ways to protect traffic over a wireless link: all the same ways traffic can be protected over a wired link. The use of secure shell (SSH) instead of telnet, secure socket layer (SSL) for web and e-mail transactions, and virtual private networks (VPN) will all make data harder to intercept.

3. 802.11x IN DEPTH

The IEEE 802.11 standard, much like other 802.x standards such as Ethernet, is designed for use in small to medium geographical distributions, such as a home, an office, a restaurant, an airline terminal, a campus, or a small town or city. It cannot be used to build, for example, a cross-country backbone or a satellite uplink. The goal of the 802.11 protocol is also similar to other link-layer protocols in that its purpose is to control access to a shared medium. In this case, the medium is radio signals transmitted through space instead of electrical impulses transmitted over copper or optical cables. A wireless network adapter is quite similar to a wired network adapter. It must carry out all the same actions as its wired counterpart; however, some of these actions are much more complicated when the wires are removed. 802.11 adapters use the same basic algorithm as Ethernet adapters:

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

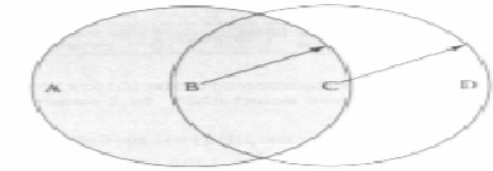
In CSMA/CD, an adapter will transmit as soon as it has data ready. If another host is found to be transmitting at the same time, a collision is said to have occurred, and both hosts will wait for a period of time and then retransmit. An Ethernet adapter resolves collisions on its shared medium by simply listening for another signal coming across the wire before its signal has reached its destination. An 802.11 adapter must have some algorithm to do the same. This presents a more complicated challenge in the wireless scenario, however, due to the fact that some nodes are not physically capable of communicating with other nodes on the network simply because they are out of transmission range. If the adapters were to just listen to the radio signals coming through the air, some collisions would not be detectable, and in other cases, adapters would remain silent even though there is no danger of collision. These two problems that arise because of the limited range of 802.11 hosts are the *hidden node* and *exposed node* problems. B can exchange information with A and C, but not D, while C can exchange information with B and D but not A. If both A and C decide that they want to communicate with B, they have no way of detecting a collision because A's signal does not reach C and C's signal does not reach A. This means that A is *hidden* with respect to C, and C is *hidden* with respect to A. On the other side of the issue, if B wants to transmit to node A, node C is aware of the transmission because it is within B's range. However, it would be incorrect of C to assume that there would be a collision if it tried to transmit to D, because that transmission wouldn't interfere with A's ability to receive from B. Thus, node C is *exposed*. In the 802.11 protocol, these problems are addressed using an algorithm called Multiple Access with Collision avoidance, or MACA. In MACA, the sender and receiver of a wireless transmission exchange a number of control frames before any data is actually transmitted. These control frames let any nearby (within range) nodes know that a transmission is occurring. First, the sender will transmit a *Request to Send* (RTS) frame to the receiver. Inside the RTS frame, there is a field that indicates how long the sender wishes to have control over the shared medium, which analogous to the length of the data within the transmission that is about to be sent. When the receiver gets an RTS, it replies with a *Clear to Send* (CTS) frame which will echo back the length field from the RTS frame back to the sender. Any node that sees the CTS frame knows that it is close to a node that is about to be receiving data, so it would know not to transmit for the duration of time specified by the length field in the CTS frame. Any node that sees the RTS frame but does not hear a CTS frame within a certain time period knows that it is far enough away from the receiver that it can transmit without worrying about interfering. In addition to the exchange of RTS and CTS frames, the receiver will also send an *acknowledgement* frame (ACK) after each frame received is successfully. Any node that is waiting to retransmit has to wait until it hears the ACK frame come across the network before it transmits.

Finally, if two nodes send an RTS frame at the same time, neither of the intended receivers will transmit a CTS frame. This will cause the senders to timeout and then use exponential back-off to calculate relatively random times to wait before retransmitting such that they won't collide again. This handshaking procedure would work well for an ad-hoc distribution of wireless nodes, but does not allow for a given node to be mobile. Certainly a static wireless network has advantages over a network consisting of hosts that are immobilized by wires, but it would clearly be more advantageous to have a protocol that would allow for hosts to move around. Luckily, the 802.11 protocol has some additional internal measures available that allow for certain nodes to be able to move freely from network to network without losing connectivity.

Fig.3 Collision with detection

Certain nodes, such as laptops and handheld computers, are considered to be *mobile nodes* and are allowed to move around freely. Other nodes, known as *access points* (AP), are connected to some underlying wired network infrastructure, or *distribution system*, and are not allowed to move. The underlying distribution system between access points can be any sort of wired networking infrastructure, such as Ethernet or FDDI. In this network configuration, even though some of the nodes are close enough to communicate with each other directly.

Fig.4 Distribution System



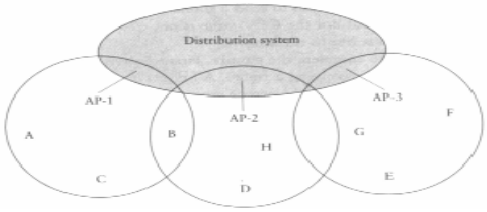
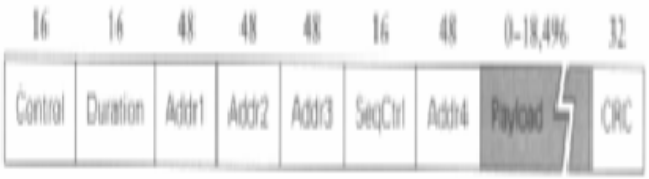


Fig.5 Frame Format for protocol 802.11x

of the nodes will communicate only with its designated access point. Therefore, if node A wants to communicate with node C, it will send information to AP-1, and AP-1 will then transmit the information to node C. If node A wants to communicate with node F, it will again send information to AP-1, and AP-1 will transmit the information to AP-3 through the distribution system. AP-3 will then wirelessly transmit the data to node F. It is important to note that the 802.11 protocol does not specify how AP-1 knew to communicate with AP-3 in order to reach node F. This information can be determined by the access points themselves using any number of external routing or bridging protocols that are not within the scope of 802.11.The 802.11 protocol's role in the formation of an access point-based wireless network is to specify how the mobile nodes determine the access point with which they should associate. The 802.11 protocol also specifies how a mobile host can roam between different access points without losing connectivity. When a mobile host comes into network or finds that its current network is not satisfactory, it engages in a process called *active scanning* by which it can determine what access point to use. First, the node sends a *Probe* frame. All access points within range will reply with a *Probe Response* frame. The mobile host will then select one of the



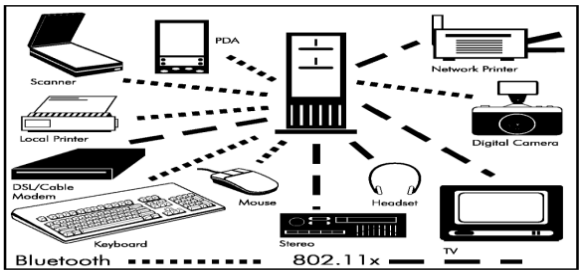
access points from which it received a response (the choice can be based on signal strength, response time, or any other criteria) and associate it self with it by sending an *Association Request* frame the access point of its choice. Finally, the access point will reply with an *Association Response* frame. When this entire process completes, the mobile node now has an access point with whom to communicate. If a node decides to move to a new location, the signal strength from its current access point will lessen and it will again engage in active scanning to find a new access point. Active scanning is not the only way a mobile host can find out about the access points in the area. Access points will periodically send out *Beacon* frames that advertise the capabilities of the access point, such as supported transmission rates. If a mobile host receives a Beacon frame from an access point that is more favorable than its current access point, it will send an Association Request frame to the new access point. This process is known as *passive scanning*. Because of the complexities introduced by the use of access points instead of direct node to node communication, an 802.11 frame is more complicated than an Ethernet frame. The Control field contains a number of subfields that are not shown in this diagram. The first is a 6-bit *Type* field that indicates if the frame is an RTS, CTS, ACK, or one of the types of frames used in the passive or active scanning algorithms. It also contains two 1-bit fields called *ToDS* and *From DS* which indicate how to interpret the four address fields. The Duration field indicates the length of the transmission. The Seq Ctrl field is used by the protocol to control the sequence of the delivery of frames. The payload is the actual data, and the CRC field contains the CRC check bits to make sure the frame is error-free. Finally, there are four separate address fields in the 802.11 frame. These addresses are interpreted based on the status of the previously mentioned *ToDS* and *From DS* bits in the control field. The reason the frame needs so many address fields is to account for the possibility that the frame could have been sent along the distribution system. If this was the case, then the frame may have been retransmitted by an access point, in which case the source address would need to reflect the fact that frame was sent by the access point and not from the original mobile host. The same reasoning can be applied to explain the need for two destination addresses. If neither of the bits is set, that means that the frame was not sent along the distribution system. In this case, *Addr1* is the address of the target node, and *Addr2* is the address of the source node. If both of the bits are set, this means that the frame has been sent from one wireless node to another wireless node, but across the distribution system. In this case, *Addr1* is the address of the final destination node, *Addr2* is the address of the access point that pulled the frame off of the distribution network on behalf of the final receiver, *Addr3* is the address of the access point that put the frame onto the distribution network on behalf of the original sender, and *Addr4* is the address of the original source. If only the *ToDS* bit is set, then the frame was put onto the distribution system by an access point but doesn't need to be taken off by another access point. This happens when a wireless host is the sender, but a wired host is the receiver. Similarly, the opposite is true when only the *From DS* bit is set. In either of these two cases, only 3 out of 4 of the addresses are used, depending on which are needed. The 802.11 protocol has been extended and adapted many times since it was originally introduced. In its first form, it was designed to run over three different physical media. Two of these types of media were radio based, and one was based on diffused infrared. One of the radio-based solutions used spread-spectrum frequency hopping to transmit data over pseudo-random radio frequencies. The other radio based solution, called *direct sequence*, dictates that both sender and receiver have a pseudorandom sequence of bits which with they encode and decode their data. Both of the original radio-based solutions ran in the 2.4 GHz frequency band of the electromagnetic spectrum. The two encoding techniques made their signals seem like noise to any receiver that didn't have the pseudorandom number with which to decode the data, and thus different hosts are able to share the same frequency range. All of the original 802.11 solutions were able to transmit at 2 megabits

Fig. 6 Different Development in Wi-Fi technology

per second, or scale down to 1 megabit per second if they were operating in a noisy RF environment. The radio solutions have ranges on the order of hundreds of feet when used indoors, while the infrared solution only had a range of about 30 feet. Since the

original 802.11 protocol went into active use, there have been numerous extensions to it. Currently, the industry leader is the 802.11b protocol; otherwise known as *Wi-Fi*. Devices using the 802.11b protocol are similar to the original 802.11 devices. 802.11b devices operate in the 2.4 GHz range and have indoor ranges on the order of hundreds of feet. 802.11b has two distinct advantages over 802.11; first, 802.11b has transmission rates of 11 megabits per second, which is a large improvement over 802.11's 2 megabits per second. Secondly, 802.11b introduced wireless encryption capability into both network adapters and access points. The next adaptation on 802.11 was 802.11a.

Hardware employing the 802.11a protocol had transmission rates of up to 54 megabits per second at frequencies in the 5 GHz range. There are many more frequency hops available in the 5 GHz range, so this 802.11a hardware was less



susceptible to interference. 802.11a hardware, however, costs about twice as much and has half the range of its 802.11b counterparts. Finally, the most recent development in wireless technology is 802.11g. This protocol operates in the 2.4 GHz frequency range, but has throughput of up to 54 megabits per second and a range that is comparable to that of 802.11b. 802.11g is also backwards compatible with 802.11b, which means that if a network has an 802.11g access point installed, users with 802.11b adapters will be able to use the network at 11 megabits per second, while users with 802.11g adapters can use the network at its full 54 megabit per second capacity. This hardware is more expensive than 802.11b hardware, but not as expensive as 802.11a hardware, making it a promising potential replacement for 802.11b once it gets out of the draft stage.

4. THINGS TO CONSIDER WHEN USING WI-Fi

Although Wi-Fi definitely has its advantages, one must take a few things into consideration when building their wireless network.

Security – By virtue of being wireless, a Wi-Fi network is less secure than a hard-wired network. Because of this it is easier for snoopers to get onto your network and possibly

access your data. Proper configuration and use of firewalls and encryption methods can help mitigate these problems.

Placement – Many cordless phones operate on the same frequency as 802.11b access points and can cause interference when used. You should also avoid placing your access point near microwave ovens for the same reason. If possible you should also find the path of least resistance from the access point to the computer, going through the least amount of walls possible.

5. CURRENT WI-FI DEVELOPMENTS

Wi-Fi has an interesting future. Currently 802.11a is being touted as the next "wireless networking solution". 802.11a is roughly five times faster, transmitting data at 54 MBps. It operates On a different frequency thus it will not encounter as much interference from cordless phones and other appliances. However, because of this the range of 802.11a is only one third that of 802.11b, transmitting only 50 feet. Using this technology will also incur a cost of roughly $100 more for the card and another $100 for the access point. Some businesses are trying to find ways to capitalize on the Wi-Fi phenomenon. For instance, Starbucks coffee shops recently announced they will be offering

Wi-Fi service in its stores, charging $3 for 15 minutes of access to $50/mo. for "unlimited minutes" with a 500 MB transfer limit, and no roaming fees. There are also social movements involved with Wi-Fi. Some believe wireless access should be free for all. These people will build more powerful amplifiers to send their signal over a larger area and allow anyone to use their signal. Some build mobile networks – cars equipped with Wi-Fi access points – and drive to areas that are in need of free Wi-Fi access. Some even engage in the practice of "war chalking", marking spots with chalk where they have discovered wireless networks so that other users may also use these networks.

6. CONCLUSION

So why should we consider using a wireless network? More than simply a fun new gadget for tech-heads to play with, there are actually many advantages to having a Wi-Fi network. For example, a home user may find it much more convenient to use his or her laptop computer in the bedroom late at night and then move it to the den during the day. A corporate user may find it very beneficial to have the freedom to work at one desk and then move to another without having to deal with networking cables. A speaker will find it very useful to simply bring their laptop to the podium and give a presentation and not have to make sure the network is set up in that particular room, deal with the cables, etc. Another main advantage is the simplicity of setting up a network. Instead of having to worry about wiring each individual desk or office to the main server room, worry about which port goes where and which ports are active, you can simply enable the access point and give the configuration to any new user that may need access to the network.

7. REFERENCES

[1] Matthew S. Gist, "802.11 Wireless Networks", The Definitive Guide, 2nd Edition, February 2005

[2] WWiSE Proposal: High throughput extension to the 802.11 Standard, January 2005. http://www.wwise.org/technicalproposal.htm

[3] TGn Sync Proposal Technical Specification, May 2005., http://www.tgnsync.org/techdocs

[4] S.M. Alamouti, "A simple transmit diversity scheme for wireless , 'communications ", IEEE J. Select. Areas Commun. vol. 16, no. 8, pp. 145 1-1458, Oct. 1998.

[5] http://en.wikipedia.org/wiki/STBC

[6] Zahed Iqbal, "Wireless LAN Technology: Current State and Future Trends", Ad Hoc Mobile Wireless Networks - Research Seminar on Telecommunication Software, Autumn2002. [8]http://en.wikipedia.org/wiki/802. 11

[7] S. Soora, K. Gosalia, M. S. Humayan, and G. Lazzi, "A comparison of two and three dimensional dipole antennas for an implantable retinal prosthesis," IEEE Trans. Antennas Propag., vol. 56, no. 3, pp. 622–629, Mar. 2008.

[8] J. Wang and D. Su, "Design of an ultra wideband system for in-body wireless communications," in Proc. 2006 4th Asia-Pacific Conf. Environmental Electromagn., Dalian, China, 2006, pp. 565–568.

[9] S. I. Kwan, K. Chang, and Y. J. Yoon, "Ultra-wide band spiral shaped