INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

WIRELESS FIDELITY

C.Suresh[1], V.Vidhya[2], J.Vishupriya[3], R.Muthulakshmi[4], S.Menaka[5]

[1]B.Tech Information Technology (Final year), vcsureshbala@gmail.com
[2] B.E Computer Science Engineering (Final year), vidhyaveeramanibe@gmail.com
[3] B.Tech Information Technology (third year), vishnu@gmail.com
[4] B.E Computer Science Engineering (third year), muthurameshcse@gmail.com
[5] B.E Computer Science Engineering (third year),smenakasengathirjkm@mail.com
Mailam Engineering College, Mailam-604304, India, 04145-241515.

Abstract: - Technology is no longer judged by its technical brilliance, but by the return on investment (both tangible and intangible). This in turn, is dictated by the killer application for that technology. Wireless Networks fit into this because the technology has been around long enough and can provide enough benefits to be seriously considered for deployment.

At the enterprise, it provides communication support for mobile computing. It overcomes and, in fact, annihilates the physical limitation of wired networks in terms of adaptability to a variation in demand.

Mobility is another feature by wireless. Mobile users can be truly mobile, in that hey don't need to be bound to their seats when connecting to the network. Mobility, however is not only associated with users, it's also associated with the infrastructure itself. You can have a wireless network up and running in no time, a boon for people who need to do it for exhibitions, events, etc.

This leads to other provision of wireless, that of scalability. It really helps in extending your network. It also becomes important if an enterprise has a rented office and needs to shift to a new place. At home, the need for wireless is more to do with ubiquitous computing.

Wi-Fi, or wireless fidelity, is freedom: it allows you to connect to the internet from your couch at home, a bed in a hotel room, or a conference room at work without wires. It is a wireless technology like cell phones, Wi-Fi enabled computers send and receive data indoors and outdoors; anywhere within the range of the base station. And the best thing of all, Wi-Fi is fast. In fact, it's several times faster than the fastest cable modem connection.

Wireless technology, therefore is really happening, and should be seriously considered. The following presentation explains wireless LANs, choice of wireless technologies., how wi-fi works?, examples & it's supporting systems, security issue , wireless-Lan configuration & finally advantages & disadvantages of wifi.

Introduction

Wi-Fi, also, **WiFi**, **WI-fi** or **wifi**, is a brand originally licensed by the Wi-Fi Alliance to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications.

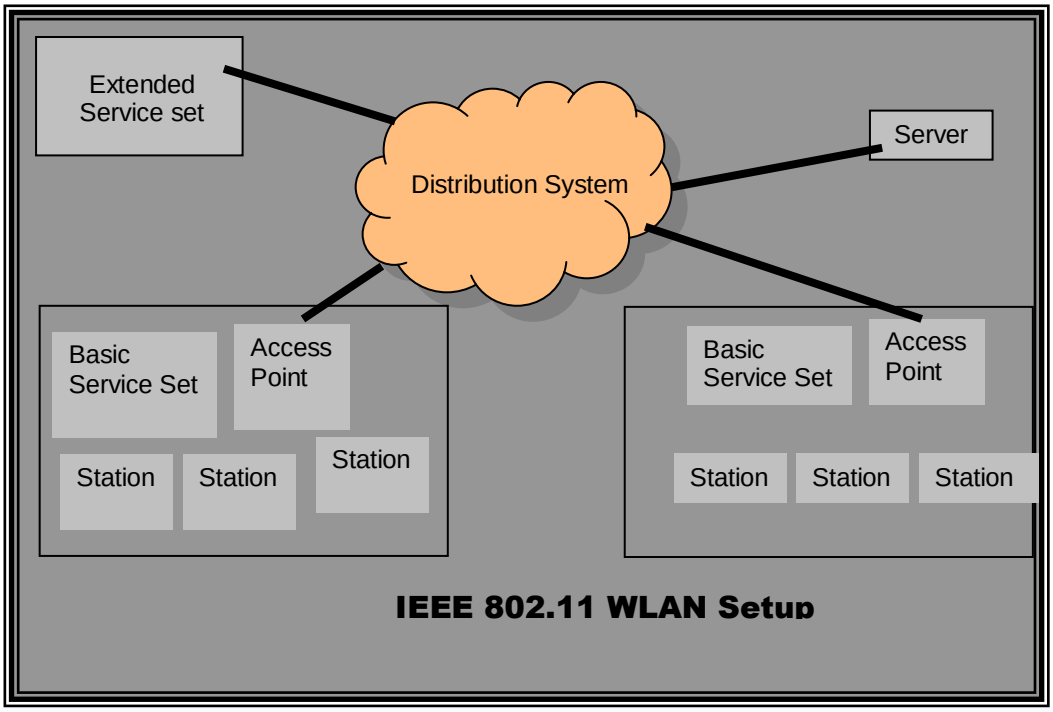
Wireless LAN (**WLAN)** is a flexible data communication system implemented as an extension to a wired LAN within a building or campus. WLANs transmit and receive data over the air by electrical signals, minimizing the need for wired connections. The advent of WLAN opened up a whole new definition of what a network

infrastructure can be. No longer does an infrastructure need to be solid and fixed, difficult to move and expensive to change. Instead it can move with the user and change as fast as the organization does.
Wi-Fi was developed to be used for mobile computing devices, such as laptops, in LANs, but is now increasingly used for more applications, including Internet and VoIP phone access, gaming, and basic connectivity of consumer electronics such as televisions and DVD players, or digital cameras. A person with a Wi-Fi device, such as a computer, telephone, or personal digital assistant (PDA) can connect to the Internet when in proximity of an access point. The region covered by one or several access points is called a hotspot. Hotspots can range from a single room to many square miles of overlapping Hotspots. Wi-Fi can also be used to create a Wireless mesh network.
Wi-Fi also allows connectivity in peer-to-peer mode, which enables devices to connect directly with each other. This connectivity mode is useful in consumer electronics and gaming applications.

Choice of Wireless Technology

The widespread reliance on networking in business and the meteoric growth of the Internet and online services are strong testimonials to the benefits of shared data and shared resources. With wireless LANs, users can access shared information without looking for a place to plug-in. Wireless LAN offers the following productivity and convenience over Wired Networks:

- ► Mobility
- ► Installation Speed and Simplicity
- ► Installation Flexibility
- ► Reduced Cost of Ownership
- ► Scalability



Wi-Fi: How it works

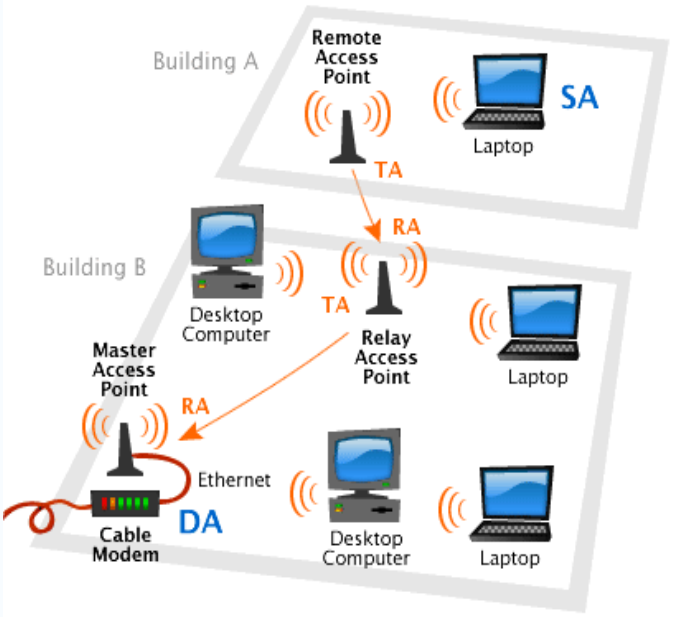
A typical Wi-Fi setup contains one or more Access Points (APs) and one or more clients. An AP broadcasts its SSID (Service Set Identifier, "Network name") via packets that are called beacons, which are broadcast every 100 ms. The beacons are transmitted at 1 Mbit/s, and are of relatively short duration and therefore do not have a significant influence on performance. Since 1 Mbit/s is the lowest rate of Wi-Fi itassures that the client who receives the beacon can communicate at least 1 Mbit/s. based on the settings (e.g. the SSID), the client may decide whether to connect to an AP. Also the firmware running on the client Wi-Fi card is of influence. Say two APs of the same SSID are in range of the client, the Firmware may decide based on signal strength to which of the two APs it will connect. The

Wi-Fi standard leaves connection criteria and roaming totally open to the client. This is strength of Wi-Fi, but also means that one wireless adapter may perform substantially better than the other. Since Wi-Fi transmits in the air, it has the same properties as a non-switched ethernet network. Even collisions can therefore appear as in non-switched Ethernet LAN's.

Channels

Except for 802.11a, which operates at 5 GHz, WI-Fi uses the spectrum near **2.**4GHz, which is standardized and *unlicensed* by international agreement; although the exact frequency allocations vary slightly in different parts of the world, as does maximum permitted power. However, channel numbers are standardized by frequency throughout the world, so authorized frequencies can be identified by channel numbers.
The frequencies for 802.11 b/g span 2.400 GHz to 2.487 GHz. Each channel is 22 MHz wide and 5 MHz spacers between the channels are required.

WORKING OF WI-FI



Examples of Standard Wi-Fi Devices

Wireless Access Point (WAP)

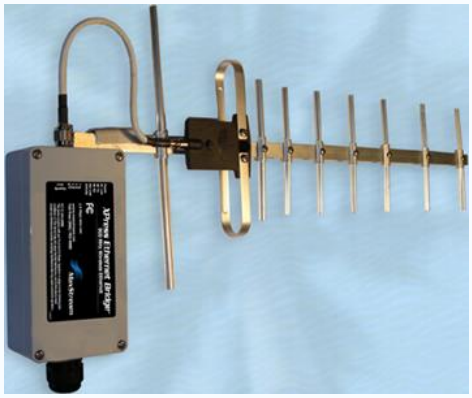
A wireless access point (AP) connects a group of wireless stations to an adjacent wired local area network (LAN). An access point is similar to an Ethernet hub, but instead of relaying LAN data only to other LAN stations, an access point can relay wireless data to all other compatible wireless devices as well as to a single (usually) connected LAN device, in most cases an ethernet hub or switch, allowing wireless devices to communicate with any other device on the LAN.

Wireless Routers

A wireless router integrates a wireless access point with an ethernet switch and an ethernet router. The integrated switch connects the integrated access point and the integrated ethernet router internally, and allows for external wired ethernet LAN devices to be connected as well as a (usually) single WAN device such as a cable modem or DSL modem. A wireless router advantageously allows all three devices (mainly the access point and router) to be configured through one central configuration utility, usually through an integrated web server. However one disadvantage is that one may not decouple the access point so that it may be used elsewhere.

Wireless Ethernet Bridge

A wireless Ethernet bridge connects a wired network to a wireless network. This is different from an access point in the sense that an access point connects wireless devices to a wired network at the data-link layer.



Two wireless bridges may be used to connect two wired networks over a wireless link, useful in situations where a wired connection may be unavailable, such as between two separate homes.

Range Extender

A wireless range extender (or wireless repeater) can increase the range of an existing wireless network by being strategically placed in locations where a wireless signal is sufficiently strong and near by locations that have poor to no signal strength. An example location would be at the corner of an L shaped corridor, where the access point is at the end of one leg and a strong signal is desired at the end of the other leg. Another example would be 75% of the way between the access point and the edge of its useable signal. This would effectively increase the range by 75%.
Wireless LANs are generally categorized according to the transmission technique that is used. Each technique comes with its own set of advantages and limitations.

They fall under the following categories:

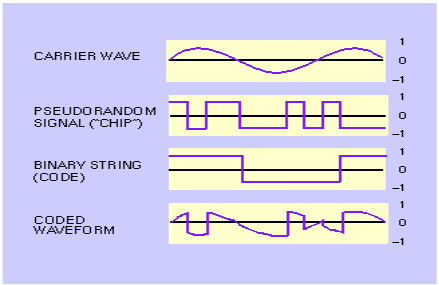
NARROW BAND TECHNOLOGY

Narrowband radio system transmits and receives user information on a specific radio frequency. Undesirable crosstalk between communication channels is avoided by carefully coordinating different users on different channel frequencies. In this system privacy and noninterference are accomplished by the use of separate radio frequencies. The receiver filters out all radio signals except the ones on its distinguished frequency.

SPREAD SPECTRUM TECHNOLOGY

Most wireless LAN systems use spread spectrum technology. Designed to trade off band-width efficiency for reliability, integrity, and security. More bandwidth is consumed as compared to Narrowband Technology but the signal produced is louder and thus easier to detect provided that the receiver knows the parameters of the spread spectrum signal being broadcast.

Figure 15 Synthesized spread spectrum information encoded by the direct sequence method



FREQUENCY HOPPING SPREAD SPECTRUM TECHNOLOGY

Frequency hopping spread spectrum (FHSS) uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver. Properly synchronized, the net effect is to maintain a single logical channel. To an unintended receiver, FHSS appears to be short-duration impulse noise.

DIRECT-SEQUENCE SPREAD SPECTRUM TECHNOLOGY

Direct-Sequence spread spectrum (DSSS) generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called **CHIP** (Chipping Code). The longer the chip the greater the probability that the original data can be recovered. To an unintended receiver, DSSS appears as low power wide band noise and is rejected by most narrowband receivers.

INFRARED TECHNOLOGY

Infrared (IR) systems use very high frequencies just below visible light in the electromagnetic spectrum to carry data. IR is either directed or diffused technology. Inexpensive directed systems provide very limited range and are used for personal area networks.

Wi-Fi and its support by operating systems

There are two sides to Wi-Fi support under an operating system. Driver level support and configuration and management support.

Driver support is usually provided by the manufacturer of the hardware or, in the case of Unix clones such as Linux and FreeBSD, sometimes through open source projects.

Configuration and management support consists of software to enumerate, join, and check the status of available Wi-Fi networks. This also includes support for various encryption methods. These systems are often provided by the operating system backed by a standard driver model. In most cases, drivers emulate an Ethernet device and use the configuration and management utilities built into the operating system. In cases where built in configuration and management support is non-existent or inadequate; hardware manufacturers may include their own software to handle the respective tasks.

Microsoft Windows

Microsoft Windows has comprehensive driver-level support for Wi-Fi, the quality of which depends on the hardware manufacturer. Hardware manufactures almost always ship Windows drivers with their products. Windows ships with very few Wi-Fi drivers and depends on the OEMs and device manufactures to make sure users get drivers. Configuration and management depend on the version of Windows.

- Earlier versions of Windows, such as 98 and ME do not have built-in configuration and management support and must depend on software provided by the manufacturer
- Microsoft Windows XP has built-in configuration and management support. The original shipping version of Windows XP included rudimentary support which was dramatically improved in Service Pack 2. Support for WPA2 and some other security protocols require updates from Microsoft. To make up for Windows inconsistent and sometimes inadequate configuration and management support, many hardware manufacturers include their own software and require the user to disable Windows' built-in Wi-Fi support
- Microsoft Windows Vista is expected to have improved Wi-Fi support over Windows XP. Current betas automatically connect to unsecured networks without the user's approval.

This is a large security issue for the owner of the respective unsecured access point and for the owner of the Windows Vista based computer because shared folders may be open to public access.

The Security Issue

One of the most frequently asked questions put to wireless local-area network (WLAN) vendors is, "**what about security?**"

The normal Wired LAN is highly secured since the communication medium is well guided by a cable usually inside a building. But that is not the case for wireless medium since the radio waves penetrate outside the building & spread out in the atmosphere, creating a risk that their network can be hacked from anywhere outside. Hence **WLAN** expects **WLAN** user to be authenticated. The designers of IEEE802.11b tried to overcome the security issue by devising a **user Authentication** and **Data Encryption** system known as **Wired Equivalent Privacy** (WEP). **WEP** has got the following properties for providing adequate security to Wireless LAN:

- ► Reasonably Strong Encryption
- ► Self Synchronizing
- ► Efficient
- ► Exportable

WEP – THEORY OF OPERATION

The process of disguising (binary) data in order to hide its information content is called encryption (denoted by E). Data that is not enciphered is called plaintext (denoted by P) and data that is enciphered is called cipher text (denoted by C). The process of turning cipher text back into plaintext is called decryption (denoted by D). A cryptographic algorithm, or cipher, is a mathematical function used for enciphering or deciphering data. Modern cryptographic algorithms use a key sequence (denoted by k) to modify their out-put. The encryption function E operates on P to produce C:

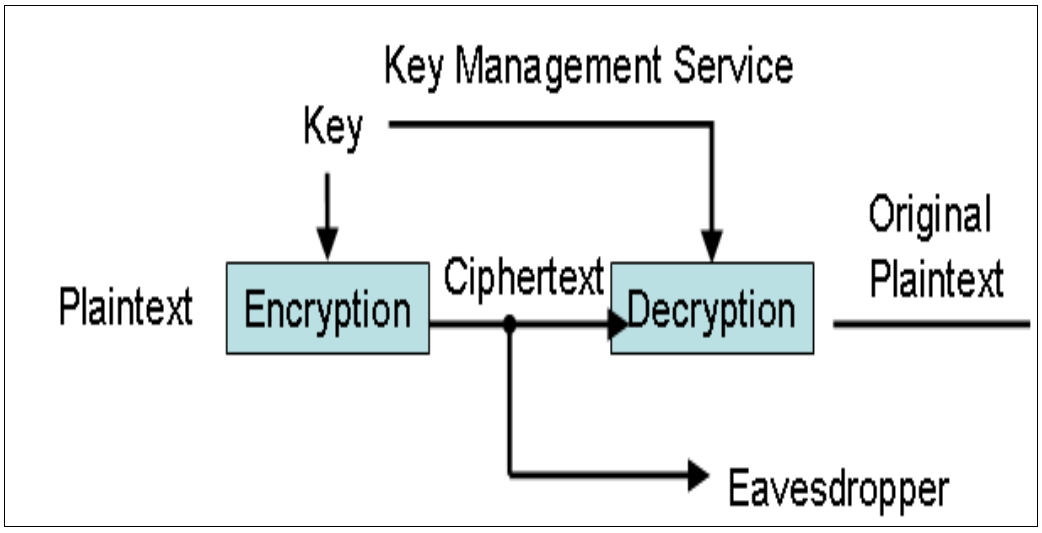
$$E_k(P) = C$$

In the reverse process, the decryption function D operates on C to produce P:

$$D_k(C) = P$$

As illustrated in the figure below, note that if the same key can be used for encryption and decryption then

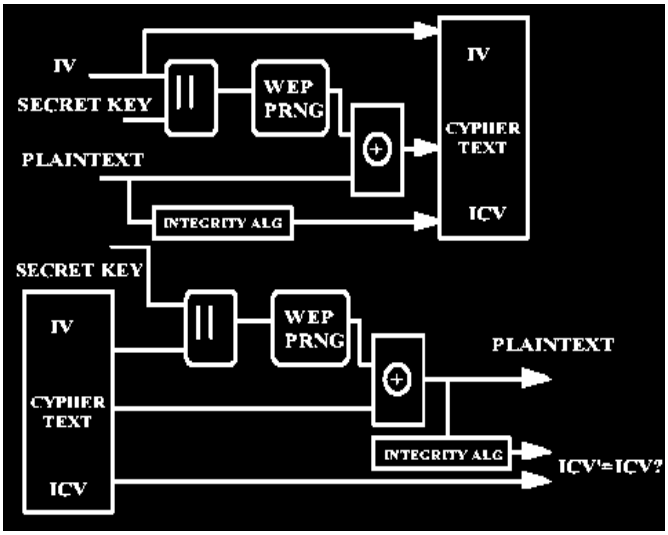
$$D_k(E_k(P)) = P$$



Generic Encryption / Decryption

Referring to above figure and viewing from left to right, encipherment begins with a **secret key** that has been distributed to cooperating STAs by an external key management service. WEP is a symmetric algorithm in which the same key is used for encipherment and decipherment.

Vol.4 Issue 2, Pg.: 50-59
February 2016



The secret key is concatenated with an **initialization vector** (IV) and the resulting **seed** is input to a PRNG. The PRNG outputs a **key sequence k** of pseudorandom octets equal in length to the number of data octets that are to be transmitted in the expanded MPDU plus 4 [since the key sequence is used to protect the **integrity check value** (ICV) as well as the data]. Two processes are applied to the plaintext MPDU. To protect against unauthorized data modification, an integrity algorithm operates on ***P*** to produce an ICV. Encipherment is then accomplished by mathematically combining the key sequence with the plaintext concatenated with the ICV. The output of the process is a **message** containing the IV and cipher text. The WEP PRNG (WEP uses the RC4 PRNG algorithm from RSA Data Security, Inc.6) is the critical component of this process, since it transforms a relatively short secret key into an arbitrarily long key sequence. This greatly simplifies the task of key distribution, as only the secret key needs to be communicated between STAs. Apart from WEP, **WLAN** security may be enhanced using several mechanisms end to end security such as Remote Authentication Dial-In User Service (RADIUS), Firewall etc. or some proprietary encryption.

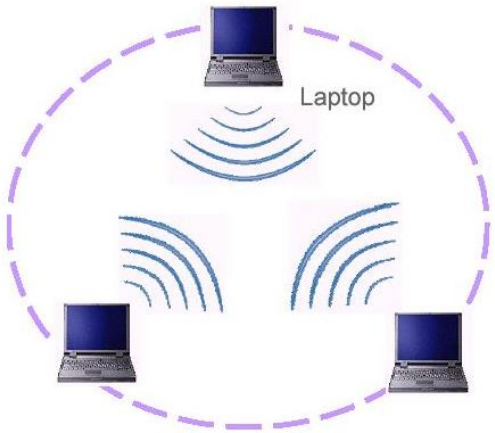
One of the standards that IEEE has drafted for enhancing security is 802.1 x which is designed to provide enhanced security for users of 802.11b WLAN.

WIRELESS-LAN CONFIGURATION

A WLAN can be configured in two basic ways:

► **Peer- to –Peer** (ad hoc mode):

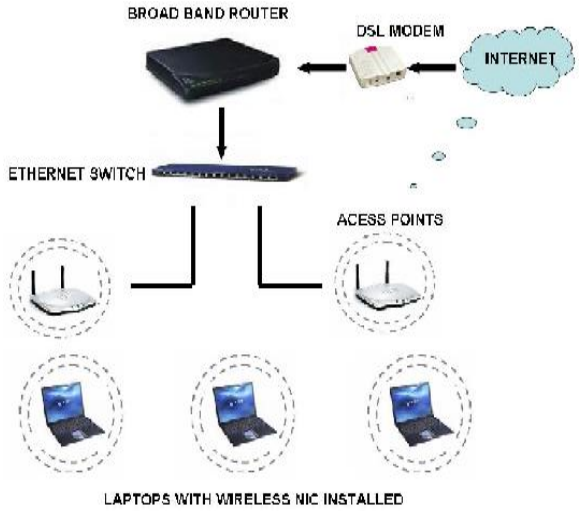
An ad hoc network is peer-to-peer network (no centralized server) set up temporarily to meet some immediate need. This mode consists of two or more PCs equipped with wireless adapter control but with no connection to a wired network.



Ad-hoc LAN

►**Client/Server(**infrastructure networking):

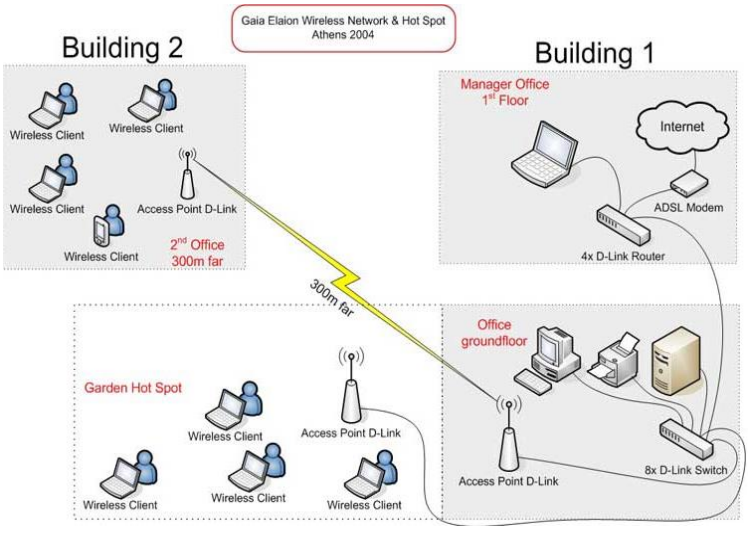
Offering fully distributed data connectivity, this mode typically consists of multiple PCs linked to a central hub that acts as a bridge to the resources of the wired network. The carrier waves transporting the data will not interfere with each other, as long as they are sent out on different frequencies. At the other end of the communication, a radio receiver tuned to a specific frequency will "hear" only the messages on that frequency. All other signals will be treated as noise and ignored. Most WLANs use the 2.4 Gigahertz (GHz) frequency band. Countries around the world have set aside this portion of the airwaves for unlicensed devices.



Infrastructure Networking

THE WLAN TOPOLOGY

The basic building block of the wireless LAN is the **cell.** This is the area in which the wireless communication takes place. The coverage area of a cell depends on the strength of the propagated radio signal and the type and construction of the walls, partitions and other physical characteristics of the indoor environment. PC-based workstations can move freely in the cell.



Wireless LAN Connectivity

Each Wireless LAN cell requires some communications traffic management. This is coordinated by an Access Point which communicates with each wireless station in its coverage area. Stations also communicate with each other via the AP so communicating stations can be hidden from one another. In this way, the AP functions as a relay, extending the range of the system.

The AP functions as a bridge between the wireless stations and the wired network and the other wireless cells. Connecting the AP to the backbone or the other wireless cells can be extended by cascading several wireless links one after the other. When any area in the building is within the reception range of more than one access point the cells' coverage is said to overlap. Each wireless station automatically establishes the best possible connection with one of the access point.

The Roaming facility allows mobile users with portable stations to move freely between overlapping cells, constantly maintaining their network connection. Roaming is seamless; a work session can be maintained while moving from one cell to another. Multiple access points can provide wireless coverage for an entire building or campus. When coverage area of two or more APs overlap, the best possible connection is established. In order to minimize packet loss during switch over, the "old" and "new" APs communicate to co-ordinate the process.

Advantages of Wi-Fi

- Allows LANs to be deployed without cabling, typically reducing the costs of network deployment and expansion. Spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.
- Wi-Fi silicon pricing continues to come down, making Wi-Fi a very economical networking option and driving inclusion of Wi-Fi in an ever-widening array of devices.
- 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. Products designated as Wi-Fi CERTIFIED by the Wi-Fi Alliance are interoperable and include WPA2 security.
- 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.
- Widely available in more than 250,000 public hot spots and millions of homes and corporate and university campuses worldwide.
- As of 2006, WPA and WPA2 encryption are not easily crackable if strong passwords are used
- New protocols for Quality of Service (WMM) and power saving mechanisms (WMM Power Save) make Wi-Fi even more suitable for latency-sensitive applications (such as voice and video) and small form-factor devices.

Disadvantages

- Wi-Fi can be interrupted by other devices, notably 2.4 GHz cordless phones.
- Power consumption is fairly high compared to some other standards, making battery life and heat a concern.
- The most common wireless encryption standard, Wired Equivalent Privacy or WEP, has been shown to be breakable even when correctly configured.
- Wi-Fi Access Points typically default to an open (encryption-free) mode. Novice users benefit from a zero configuration device that works out of the box but might not intend to provide open wireless access to their LAN. WPA Wi-Fi Protected Access which began shipping in 2003 aims to solve these problems and is now generally available, but adoption rates remain low. .
- Wi-Fi networks can be monitored and used to read and copy data (including personal information) transmitted over the network when no encryption such as VPN is used.
- Interoperability issues between brands or deviations from the standard can disrupt connections or lower throughput speeds on other user's devices within range. Wi-Fi Alliance programs test devices for interoperability and designate devices which pass testing as Wi-Fi CERTIFIED.

Conclusion

In this article we have learnt how, essentially, Wi-Fi is really for when cabling is not a feasible option and Bluetooth is for intercommunication between devices without the need for a PC. Bluetooth makes connecting various devices to each other without the need for cables a fairly easy task, whereas 802.11-based products can extend, or replace, a wired Local Area Network. From a personal user's point-of-view, I would suggest - if possible - having both available if you're everyday life requires you to travel to different destinations and meet different people. This way you will always be ready, if one isn't available then you can use the other.

It's no secret that the overall performance of a wired LAN is more superior to a wireless network. However, expect improvements, in the coming years things will get bigger and better. Having said this, the word that comes to my mind when I think of wireless - especially Wi-Fi - is *Convenience*. This technology makes sitting out on the porch or in the garden on a hot summer's day and browsing the Internet a possibility.

REFERENCES

[1] M.sauer,A.Kobyakov,and J.George, "Radio over fiber for picocellular network architecture ,"Lighwave Technology ,journal of ,Vol.25,no.11,pp.3301-3320,Nov.2007.

[2] T.Rappaport,Wireless Communications principles an practice .Upper Saddle River ,"NJ:prentice Hall,1999.

[3] COST 231,"Digital mobile radio towards future generation systems, "European Commision,Brussels,Belgium,Tech.Rep,1999.

[4] "Iperf software."[Online].Available:http://iperf.sourceforge.net/%http://dast.nlanr.net.

[5] I.Haratcherev,C.Balageas,and M.Fiorito,"Low consumption home femto base stations ,"in personal ,indoor and mobile radio communication,2009 IEEE 20th International symposium on.2009.pp.1_5.