en
cs de
sk es

TECH
pedia

WIRELESS NETWORKS

JORDI SALAZAR

Title: Wireless networks
Author: Jordi Salazar
Published by: Czech Technical University of Prague
Faculty of electrical engineering
Contact address: Technicka 2, Prague 6, Czech Republic
Phone Number: +420 224352084
Print: (only electronic form)
Number of pages: 37
Edition: 1st Edition, 2017

ISBN 978-80-01-06197-8

TechPedia
European Virtual Learning Platform for
Electrical and Information Engineering

http://www.techpedia.eu

This project has been funded with support from the European Commission.
This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Explanatory Notes

	Definition
	Interesting
	Note
	Example
	Summary
	Advantage
	Disadvantage

ANNOTATION

This module provides an introduction to wireless networks in general and wireless LANs in particular. It describes and explains what the different wireless technologies are, their main features, security issues, advantages, disadvantages and uses or applications.

OBJECTIVES

Learn architectural differences of various wireless networks. Learn about security aspects of wireless networks. Know pros and cons of wireless networks.

LITERATURE

[1] William Stallings, Wireless Communications and Networks, Second Edition, Pearson Prentice Hall, Upper Saddle River, NJ, 2005. ISBN 0-13-191835-4.

[2] B. Ciubotaru, G.M. Muntean, *Advanced Network Programming. Principles and Techniques*, Springer-Verlag London, 2013. ISBN 978-1-4471-5292-7.

[3] K. Sharma, N. Dhir, "A study of wireless networks: WLANs, WPANs, WMANs, and WWANs with comparison", *International Journal of Computer Science and Information Technologies*, vol. 5 (6), pp. 7810-7813, 2014.

[4] K. Pothuganti, A. Chitneni, "A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", *Advance in Electronic and Electric Engineering*, vol. 4 (6), pp. 655-662, 2014.

[5] "An introduction to Wi-Fi", Rabbit product manual, Digi International Inc., 2007-2008. (www.rabbit.com)

[6] IEEE Standards Association web site (http://standards.ieee.org/index.html).

Index

1 Introduction to wireless networks

This module provides an introduction to wireless networks in general and wireless LANs in particular. It describes and explains what the different wireless technologies are, their main features, security issues, advantages, disadvantages and uses or applications.

Wireless networks are networks that use radio waves to connect devices, without the necessity of using cables of any kind.

Devices commonly used for wireless networking include portable computers, desktop computers, hand-held computers, personal digital assistants (PDAs), cellular phones, pen-based computers, and pagers. Wireless networks work similar to wired networks, however, wireless networks must convert information signals into a form suitable for transmission through the air medium.

Wireless networks serve many purposes. In some cases they are used as cable replacements, while in other cases they are used to provide access to corporate data from remote locations.

Wireless infrastructure can be built for very little cost compared to traditional wired alternatives. But building wireless networks is only partly about saving money. By providing people in your local community with cheaper and easier access to information, they will directly benefit from what the Internet has to offer. The time and effort saved by having access to the global network of information translates into wealth on a local scale, as more work can be done in less time and with less effort.

Wireless networks allow remote devices to connect without difficulty, independently these devices are a few feet or several kilometers away. And no need to break through walls to pass cables or install connectors. This has made the use of this technology very popular, spreading rapidly.

There are many different technologies that differ in the transmission frequency used, speed and range of their transmissions.

On the other hand, there are some issues related to the legal regulation of the electromagnetic spectrum. Electromagnetic waves are transmitted through many devices, but are prone to interference. For this reason, all countries need regulations that define the frequency ranges and transmission power for each technology is permitted.

In addition, electromagnetic waves are not easily confined to a restricted geographic area. For this reason, a hacker can easily listen to a network if the data transmitted are not encoded. Therefore, all necessary steps should be taken to ensure the privacy of data transmitted over wireless networks

2 Wireless technologies

Wireless networks can be classified into four specific groups according to the area of application and the signal range [1-3]: Wireless Personal-Area Networks (WPAN), Wireless Local-Area Networks (WLANs), Wireless Metropolitan-Area Networks (WMAN), and Wireless Wide-Area Networks (WWANs). Figure 1 illustrates these four categories.

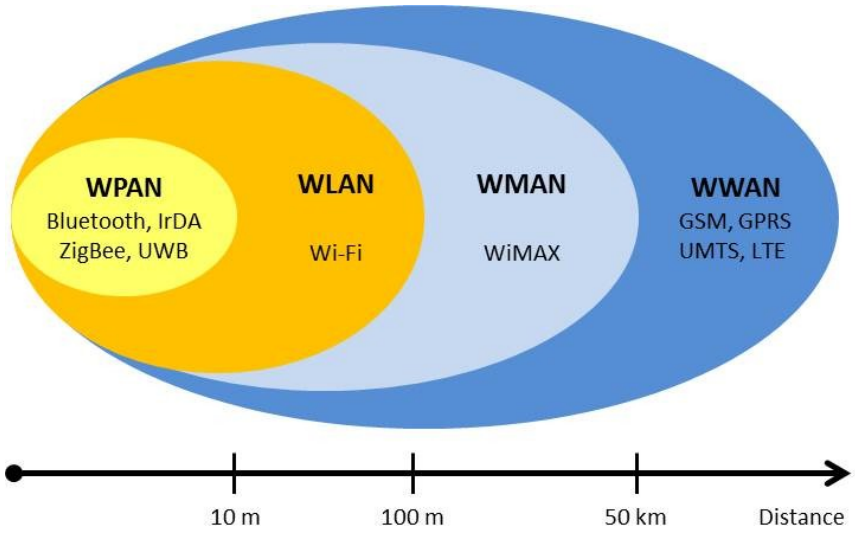

Fig. 1.1 Wireless networks classification

In addition, wireless networks can be also divided into two broad segments: short-range and long-range. Short-range wireless pertains to networks that are confined to a limited area. This applies to local area networks (LANs), such as corporate buildings, school campuses, manufacturing plants or homes, as well as to personal area networks (PANs) where portable computers within close proximity to one another need to communicate. These networks typically operate over unlicensed spectrum reserved for industrial, scientific and medical (ISM) usage. The available frequencies differ from country to country. The most common frequency bands are at 2.4 GHz and at 5 GHz, which are available across most of the globe. The availability of these frequencies allows users to operate wireless networks without obtaining a license, and without charge. As a license is not required for use, this has facilitated the expansion of such networks.

In long-range networks, connectivity is typically provided by companies that sell the wireless connectivity as a service. These networks span large areas such as a metropolitan area (WMAN), a state or province, or an entire country. The goal of long-range networks is to provide wireless coverage globally. The most common long-range network is wireless wide area network (WWAN). When true global coverage is required, satellite networks are also available.

2.1 Wireless Personal-Area Networks (WPAN)

Wireless Personal Area Networks are based on the IEEE 802.15 [http://en.wikipedia.org/wiki/IEEE_802.15] standard [3-4]. They permit communication in a very short range, of about 10 meters. Unlike other wireless networks, a connection made through a WPAN involves little or no infrastructure or direct connectivity to the world outside the link. This allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices such as a smartphone and a PDA.

These networks are characterized by low power demands and a low bit rate. Such kind of networks relay on technologies such as Bluetooth, IrDA, ZigBee or UWB. From an application point of view, Bluetooth is intended for a cordless mouse, keyboard, and hands-free headset, IrDA is intended for point-to-point links between two devices for simple data transfers and file synchronization, ZigBee is designed for reliable wirelessly networked monitoring and control networks and, UWB is oriented to high-bandwidth multimedia links.

Bit Rate is the number of bits transferred or received per unit of time (Unit: bps or bit/s)

A **Modem** is a device that enables a computer to transmit and receive data

- **Bluetooth**

Bluetooth corresponds to the IEEE 802.15.1 standard. Originally Bluetooth was designed for low power consumption, short range and omni-directional (point to multipoint) communications, and cheap devices, to be used as a cable replacement, linking devices through an ad hoc connection of radio waves. Nowadays developers are designing Bluetooth-enabled components and systems for a range of additional applications. This technology operates for three different classes of devices: Class 1, class 2 and class 3 where the range is about 100 meters, 10 meters and 1 meter respectively. Using the 2.4 GHz band, two devices within the coverage range of each other can share up to 720 Kbps of capacity or transfer rate. The most commonly used is class 2.

A Bluetooth network is also called a piconet, and is composed of up to 8 active devices in a master-slave relationship. The first Bluetooth device in the piconet is the master, and all other devices are slaves that communicate with the master. A piconet typically has a range of 10 meters, although ranges of up to 100 meters can be reached under ideal circumstances. To provide security, each link is encoded and protected against eavesdropping and interference. Two piconets can be connected to form a scatternet. A Bluetooth device may participate in several piconets at the same time, thus allowing for the possibility that information could flow beyond the coverage area of the single piconet. A device in a scatternet could be a slave in several piconets, but master in only one of them.

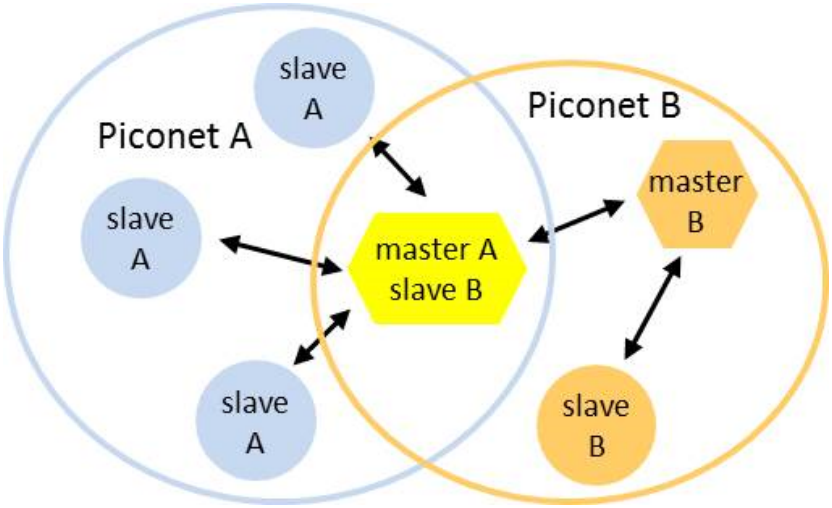

Fig. 1.2 Bluetooth scatternet comprising two piconets. The Master in piconet A is a slave in piconet B.

- **IrDA**

The Infrared Data Association (IrDA) specifies a complete set of infrared communications standards. IrDA refers to that set of standards and is used to provide wireless connectivity to devices that would normally use cables for connectivity. IrDA is a low-power, low-cost, unidirectional (point to point), narrow angle (< 30º) cone, ad hoc data transmission standard designed to operate over a distance of up to 1 meter and at speeds of 9600 bps to 4 Mbps (currently), 16 Mbps (under development). Some of the devices that use IrDA are notebooks, PDAs, printers and cameras.

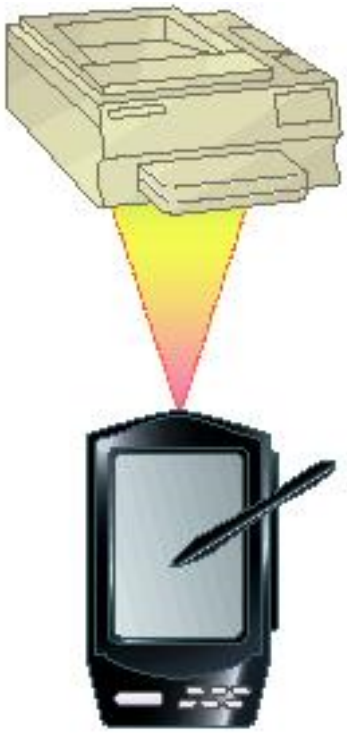

Fig. 2 . IrDA communication between a PDA and a printer (point to point)

- **ZigBee**

ZigBee is based on the IEEE 802.15.4 standard and was developed as an open global standard to address the unique needs of easy implementation, high reliability, low-cost, low-power and low-data rate wireless device networks. ZigBee operates the unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz at a maximum transfer rate of 250 Kbps, enough to satisfy sensor and automation needs using wireless.

ZigBee also serves for creating larger wireless networks not demanding high data throughput. Two different device types can participate in a ZigBee network: Full-function devices (FFD) and reduced-function devices (RFD). FFDs can operate in three modes serving as a WPAN coordinator, coordinator or device. RFD is only intended for applications that are extremely simple, such as a light switch. ZigBee supports three different topologies: star, mesh, and cluster tree, which are shown in Figure 1.4. In the star topology, the communication is established between devices and a single central controller, called the WPAN coordinator. In the mesh topology, any device can communicate with any other device as long as they are in range of one another. Cluster-tree network is a special case of a mesh network in which most devices are FFDs and a RFD may connect to a cluster-tree network as a leaf node at the end of a branch. Any of the FFD can act as a router and provide synchronization services to other devices and routers. Only one of these routers is the WPAN coordinator.

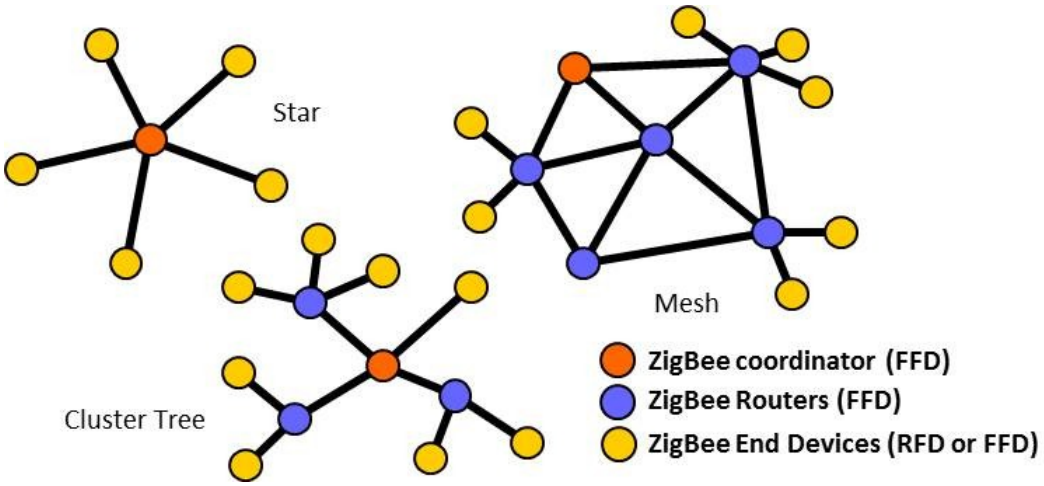

Figure 1.4 ZigBee network structure diagram

- **UWB**

Based on the IEEE 802.15.3 standard, Ultra Wide Band (UWB) technology has recently attracted much attention as an indoor short-range high-speed wireless communications. UWB serves a very different purpose than the other technologies mentioned in this section. UWB enables the movement of massive files at high data rates over short distances. Thus, UWB has a data transfer over 110 Mbps up to 480 Mbps at distances up to few meters which can satisfy most of the multimedia applications such as audio and video delivery in home networking and it can also act as a wireless cable replacement of high speed serial bus such as USB 2.0 and IEEE 1394. In America, frequencies for UWB have been allocated in the 3.1 GHz

to 10.6 GHz band. However, in Europe, the frequencies include two parts: from 3.4 GHz to 4.8 GHz and 6 GHz to 8.5 GHz.

UWB transmissions transmit information by generating radio energy at specific time intervals and occupying a large bandwidth, see Figure 1.5, thus enabling pulse-position or time modulation. The information can also be modulated on UWB signals (pulses) by encoding the polarity of the pulse, its amplitude and/or by using orthogonal pulses. UWB pulses can be sent sporadically at relatively low pulse rates to support time or position modulation, but can also be sent at rates up to the inverse of the UWB pulse bandwidth.

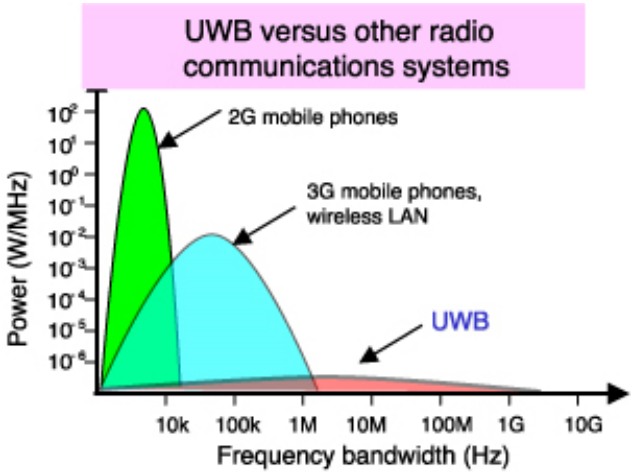

Figure 1.5 UWB power and frequency bandwidth usage.

2.2 Wireless Local-Area Network (WLAN)

Wireless Local Area Networks (WLANs) are designed to provide wireless access in areas with a typical range up to 100 meters and, are used mostly in home, school, computer laboratory, or office environments (Figure 1.6). This gives users the ability to move around within a local coverage area and still be connected to the network [2,5]. WLANs are based on IEEE 802.11standards, marketed under the Wi-Fi brand name. Due to competition, other standards such as HiperLAN never received much commercial implementation. IEEE 802.11 was simpler to implement and made it faster to the market. The complete family will be revised in more detail in section 4.

The IEEE 802.11 is a family of different standards for wireless local area networks. The IEEE 802.11b was the first accepted standard, supporting up to 11 Mbps in the 2.4 GHz unlicensed spectrum band. Then, the IEEE 802.11g standard was designed as a higher-bandwidth successor to the IEEE 802.11b. An IEEE 802.11g access point will support 802.11b and 802.11g clients. Similarly, a laptop with an IEEE 802.11g card will be able to access existing 802.11b access points as well as new 802.11g access points. That is because wireless LANs based on 802.11g will use the same 2.4-GHz band that 802.11b uses. The maximum transfer rate for the IEEE 802.11g wireless link is 54 Mbps, but it will automatically back down from 54 Mbps when the radio signal is weak or when interference is detected.

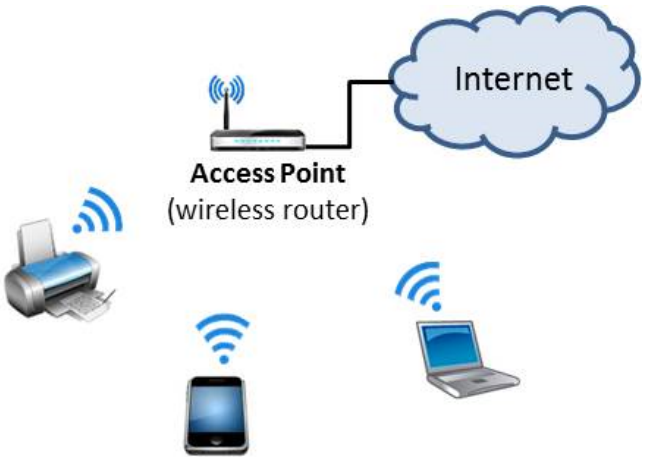

Figure 1.6 Home WLAN diagram

2.3 Wireless Metropolitan-Area Network (WMAN)

Wireless Metropolitan Area Networks (WMANs) is the third group of wireless networks. WMANs are based on IEEE 802.16 standard which is often called WiMAX (Worldwide Interoperability for Microwave Access). WiMAX is a communications technology that supports point to multipoint architecture aimed at providing high-speed wireless data over metropolitan area networks [1-3]. This enables smaller wireless LANs to be interconnected by WiMAX creating a large WMAN. Thus, networking between cities can be achieved without the need for expensive cabling.

WiMAX is similar to Wi-Fi, but provides coverage over greater distances. While Wi-Fi is intended to provide coverage over relatively small areas, such as in offices or hot spots, WiMAX operates on two frequency bands, a mixture of licensed and unlicensed band, from 2 GHz to 11 GHz and from 10 GHz to 66 GHz, and can transfer around 70 Mbps over a distance of 50 km to thousands of users from a single base station, as depicted in Figure 1.7. As it can operate in two frequency bands WiMAX can work by line-of-sight and non-line-of-sight. At the 2 to 11GHz frequency range it works by non-line-of-sight, where a computer inside a building communicates with a tower/antenna outside the building. Short frequency transmissions are not easily disrupted by physical obstructions. Higher frequency transmissions are used for line-of-sight service. This enables to towers/antennae to communicate with each other over a greater distance.

Figure 1.7 WiMaX network diagram

2.4 Wireless Wide-Area Network (WWAN)

Wireless Wide Area Networks extend beyond 50 kilometers and typically use licensed frequencies. These types of networks can be maintained over large areas, such as cities or countries, via multiple satellite systems or antenna sites looked after by an internet services provider. There are mainly two available technologies: Digital cellular telephony and Satellites [1-3].

- **Cellular telephone networks**

In the cellular system, the coverage area is divided into cells. A cell transmitter, at center of the cell, is designed to serve an individual cell. All transmitters are connected to a base station and these latter to a mobile telecommunications switching office which links the cellular and the wired telephone network. The system seeks to make efficient use of available channels by using low-power transmitters to allow frequency reuse at much smaller distances.

Different cellular generations have been developed since early 1980s. First generation, 1G, was analog and, conceived and designed purely for voice calls with almost no consideration of data services, with a speed of up to 2.4 kbps. The second generation, 2G, was based on digital technology and network infrastructure (GSM), enabling text messages, and with a data speed of up to 64 Kbps. The 2.5G generation was between the second and the third. Sometimes it has been referred as 2G + GPRS, it is an enhanced version of 2G, with a speed of up to 144 Kbps. The 3G generation was introduced in year 2000, with a data speed of up to 2 Mbps. The 3.5G is an enhanced version of the 3G that uses HSDPA to speed data transfers up to 14 Mbps. Finally the fourth generation, 4G, is capable of providing up to 1 Gbps speed and any kind of service at any time as per user requirements, anywhere. The 5G generation is expected by year 2020.

- **Satellite**

Wireless communications can also be developed via satellite. Due to its high altitude, satellite transmissions can cover a wide area over the surface of the earth. This can be very useful for users who are located in remote areas or islands where no submarine cables are in service. In these cases, satellite telephones are needed.

Each satellite is equipped with various transponders consisting of a transceiver and an antenna. The incoming signal is amplified and then rebroadcast on a different frequency.

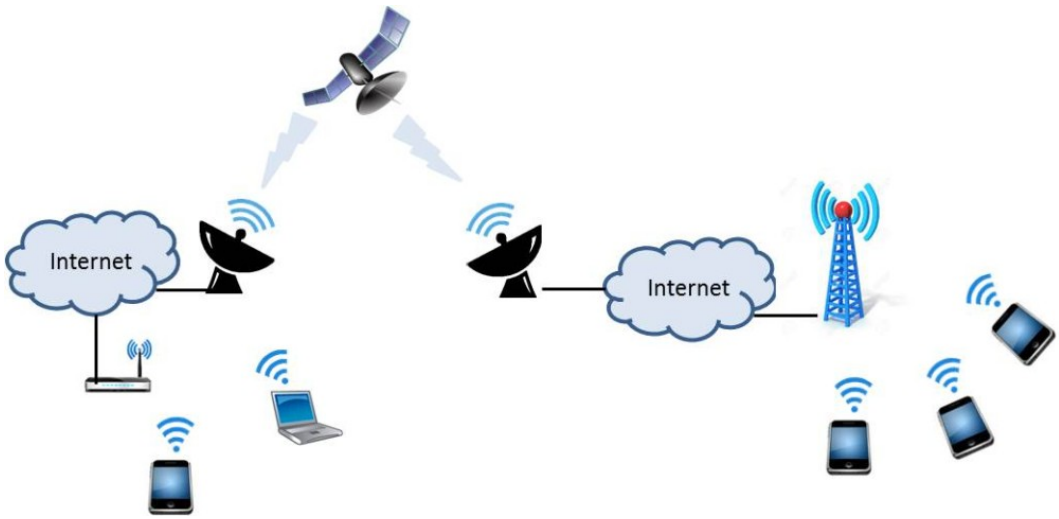

Figure 1.8 Satellite and cellular networks

3 Network architecture

3.1 Terms and terminology

This section provides definition for various terms used in a wireless network architecture. However, not all entries from a generic architecture exist in all technologies and the exact functionality may be different.

The 802.11 logical architecture contains several main components: station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS). Some of the components of the 802.11 logical architecture map directly to hardware devices, such as STAs and wireless APs. The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity. The wireless AP functions as a bridge between the wireless STAs and the existing network backbone for network access.

A **station (STA)** might be a PC, a laptop, a PDA, a phone or whatever device having the capability to interfere the wireless medium.

An **access point (AP)**, sometimes called a **base station (BS)**, is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards.

A **basic service set (BSS)** consists of an access point together with all associated STAs. The AP acts as a master to control the STAs within that BSS. The simplest BSS is composed of one AP and one STA.

An **extended service set (ESS)** is a set of one or more interconnected basic service sets (BSSs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs.

When all of the stations in the BSS are mobile stations and there is no connection to a wired network, the BSS is called an **independent BSS (IBSS).** An IBSS is an ad hoc network that contains no access points, which means they cannot connect to any other basic service set.

A **distribution system (DS)** is the mechanism by which APs exchange frames with one another and with wired networks, if any. DS is not necessarily a network, and the IEEE 802.11 standard does not specify any particular technology for the DS. In nearly all commercial products, wired Ethernet is used as the backbone network technology.

Figure 1.9 Independent and infrastructure basic service sets (BSSs).

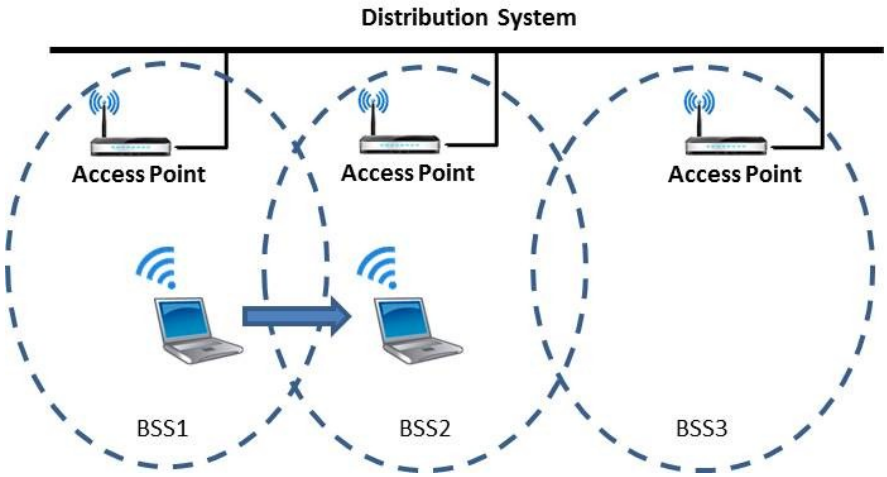

Figure 1.10 Extended service set (ESS) and mobility support.

3.2 Architectures

In wireless networks there are two modes for configuring a wireless architecture, ad hoc and infrastructure [1-2]. In Ad hoc mode, devices transmit directly peer-to-peer while on in infrastructure mode, devices communicate through an access point that serves as a bridge to other networks.

Ad hoc mode

By using ad hoc mode, all devices in the wireless network are directly communicating with each other in peer to peer communication mode (point-to-point). The network has no structure or fixed points. No access point is required for communication between devices.

Ad hoc mode is most suitable for small group of devices and all of these devices must be physically present in close proximity with each other. The performance of network suffers while the number of devices grows. Disconnections of random device may occur frequently and also, ad hoc mode can be a tough job for network administrator to manage the network. Ad hoc mode has another limitation is that, ad hoc mode networks cannot bridge to wired local area network and also cannot access internet if without the installation of special gateways.

However, ad hoc mode works fine in small environment and provides the easiest and least expensive way to set up a wireless network.

Infrastructure mode

The other architecture in wireless network is infrastructure mode. All devices are connected to wireless network with the help of an access point (AP). Wireless access points are usually routers or switches which convert airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless users. Connecting multiple access points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one access point domain to another and still maintain seamless network connection.

The infrastructure mode provides improved security, ease of management, and much more scalability and stability. However, the infrastructure mode incurs extra cost in deploying access points such as routers or switches.

Extended Service Set Identifier (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the ESSID is used, but may still be referred to as SSID.

A **service set identification (SSID)** is a 32-character (maximum) alphanumeric key identifying the name of the wireless local area network.

Some vendors refer to the SSID as the network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

4 The IEEE 802.11 standard

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area networks in the 2.4, 5, and 60 GHz frequency bands [1-2].

They are created and maintained by the IEEE 802.11 working group. The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand.

4.1 802.11 Protocol

The IEEE 802 standards committee defines two separate layers, the Logical Link Control (LLC) and media access control (MAC), for the Data-Link layer of the OSI reference model. The IEEE 802.11 wireless standard defines the specifications for the physical layer and the media access control (MAC) layer that communicates up to the LLC layer, as shown in Figure 1.11.

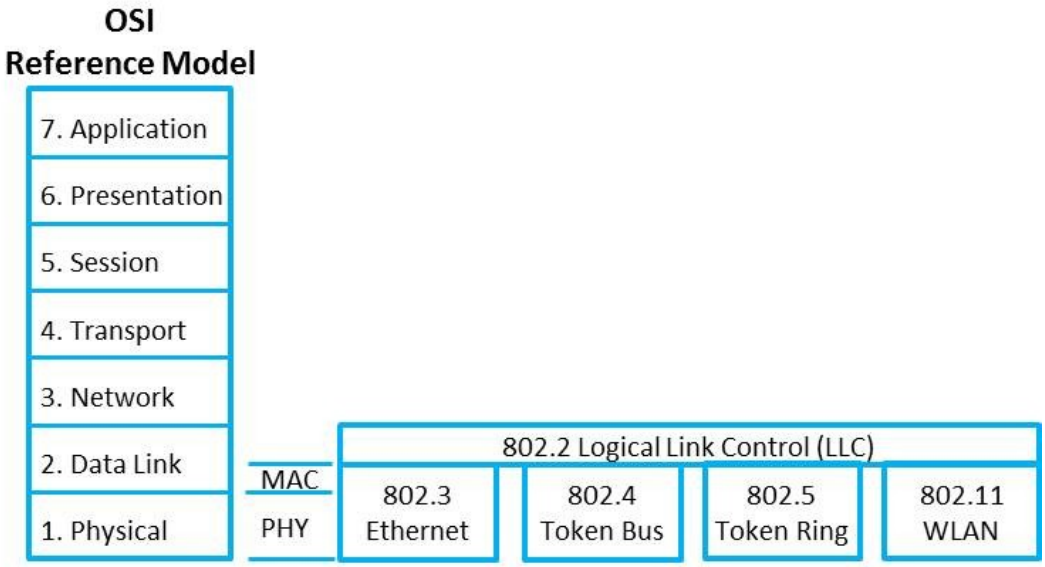

Figure 1.11The IEEE 802.11 standard and the OSI reference model

All of the components in the 802.11 architecture fall into either the media access control (MAC) sublayer of the data-link layer or the physical layer (PHY).

4.2 802.11 MAC Frame

The IEEE 802.11 standard MAC frame, as shown in Figure 1.12, consists of a MAC header, the frame body, and a frame check sequence (FCS). The MAC frame format comprises a set of nine fields that occur in a fixed order in all frames.

Frame Control Field

The Frame Control Field, see Figure 1.12, contains control information used for defining the type of 802.11 MAC frame and providing information necessary for the following fields to understand how to process the MAC frame.

A description of each Frame Control field subfield is given below:

- **Protocol Version** provides the current version of the 802.11 protocol used. Receiving STAs use this value to determine if the version of the protocol of the received frame is supported.
- **Type and Subtype** determines the function of the frame. There are three different frame type fields: control, data, and management. There are multiple subtype fields for each frame type. Each subtype determines the specific function to perform for its associated frame type.
- **To DS and From DS** indicates whether the frame is going to or exiting from the DS (distributed system), and is only used in data type frames of STAs associated with an AP.
- **More Fragments** indicates whether more fragments of the frame, either data or management type, are to follow.
- **Retry** indicates whether or not the frame, for either data or management frame types, is being retransmitted.
- **Power Management** indicates whether the sending STA is in active mode or power-save mode.
- **More Data** indicates to a STA in power-save mode that the AP has more frames to send. It is also used for APs to indicate that additional broadcast/multicast frames are to follow.
- **WEP** indicates whether or not encryption and authentication are used in the frame. It can be set for all data frames and management frames, which have the subtype set to authentication.
- **Order** indicates that all received data frames must be processed in order.

Duration/ID Field

This field is used for all control type frames, except with the subtype of Power Save (PS) Poll, to indicate the remaining duration needed to receive the next frame

transmission. When the sub-type is PS Poll, the field contains the association identity (AID) of the transmitting STA.

Address Fields

Depending upon the frame type, the four address fields will contain a combination of the following address types:

- **BSS Identifier (BSSID)** uniquely identifies each BSS. When the frame is from an STA in an infrastructure BSS, the BSSID is the MAC address of the AP. When the frame is from a STA in an IBSS, the BSSID is the randomly generated, locally administered MAC address of the STA that initiated the IBSS.
- **Destination Address (DA)** indicates the MAC address of the final destination to receive the frame.
- **Source Address (SA)** indicates the MAC address of the original source that initially created and transmitted the frame.
- **Receiver Address (RA)** indicates the MAC address of the next immediate STA on the wireless medium to receive the frame.
- **Transmitter Address (TA)** indicates the MAC address of the STA that transmitted the frame onto the wireless medium.

For more information about the address types and the contents of the address fields in the 802.11 MAC header, see the IEEE 802.11 standard at the IEEE Web site [6].

Sequence Control

The Sequence Control field contains two subfields, the Fragment Number field and the Sequence Number field, as shown in Figure 1.12.

A description of each Sequence Control field subfield is as follows:

- **Sequence Number** indicates the sequence number of each frame. The sequence number is the same for each frame sent for a fragmented frame; otherwise, the number is incremented by one until reaching 4095, when it then begins at zero again.
- **Fragment Number** indicates the number of each frame sent of a fragmented frame. The initial value is set to 0 and then incremented by one for each subsequent frame sent of the fragmented frame.

Frame Body

The frame body contains the data or information included in either management type or data type frames.

Frame Check Sequence

The transmitting STA uses a cyclic redundancy check (CRC) over all the fields of the MAC header and the frame body field to generate the FCS value. The receiving STA then uses the same CRC calculation to determine its own value of the FCS field to verify whether or not any errors occurred in the frame during the transmission.

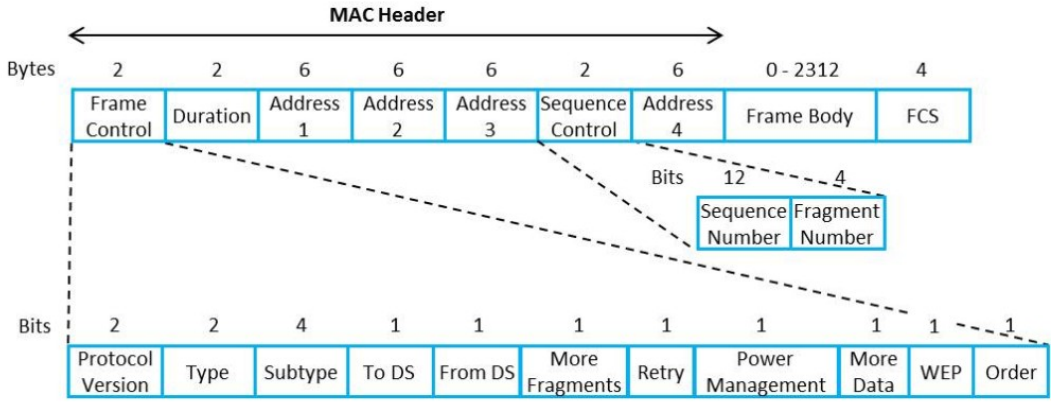

Figure 1.12 The 802.11 standard MAC frame format. Frame control and sequence control fields are detailed.

4.3 802.11 PHY Sublayer

At the physical (PHY) sublayer, IEEE 802.11 defines a series of encoding and transmission schemes for wireless communications, the most common of which are the Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Orthogonal Frequency Division Multiplexing (OFDM) transmission schemes. Figure 1.13 shows the 802.11, 802.11b, 802.11a, 802.11g, 802.11n and 802.11ac standards that exist at the PHY sublayer. These standards are described in the following sections.

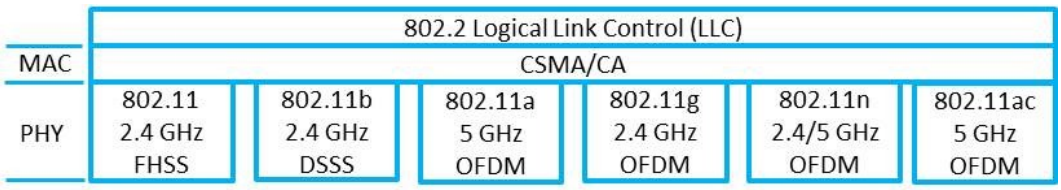

Figure 1.13 IEEE 802.11standards at the PHY layer

IEEE 802.11

The bit rate for the original IEEE 802.11 standard is 2 Mbps using the FHSS transmission scheme and the ISM frequency band, which operates in the frequency range of 2.4 to 2.5 GHz. However, under less than ideal conditions, a lower bit rate speed of 1 Mbps is used.

802.11b

The major enhancement to IEEE 802.11 by IEEE 802.11b is the standardization of the physical layer to support higher bit rates. IEEE 802.11b supports two additional speeds, 5.5 Mbps and 11 Mbps, using the 2.4 GHz frequency band. The DSSS transmission scheme is used in order to provide the higher bit rates. The bit rate of 11 Mbps is achievable in ideal conditions. In less than ideal conditions, the slower speeds of 5.5 Mbps, 2 Mbps, and 1 Mbps are used.

It is important to note that 802.11b uses the same frequency band as that used by microwave ovens, cordless phones, baby monitors, wireless video cameras, and Bluetooth devices.

802.11a

The IEEE 802.11a operates at a bit rate as high as 54 Mbps and uses the 5 GHz frequency band. Instead of DSSS, 802.11a uses OFDM, which allows data to be transmitted by subfrequencies in parallel and provides greater resistance to interference and greater throughput. This higher speed technology enables wireless LAN networking to perform better for video and conferencing applications.

Because they are not on the same frequencies as other devices (such as cordless phones that work at the 2.4 GHz frequency band), OFDM and IEEE 802.11a

provide both a higher data rate and a cleaner signal. The bit rate of 54 Mbps is achievable in ideal conditions. In less than ideal conditions, the slower speeds of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps are used.

802.11g

IEEE 802.11g operates at a bit rate as high as 54 Mbps, but uses the 2.4 GHz frequency band and OFDM. 802.11g is also backward compatible with 802.11b and can operate at the 802.11b bit rates and use DSSS. 802.11g wireless network adapters can connect to an 802.11b wireless AP, and 802.11b wireless network adapters can connect to an 802.11g wireless AP. Thus, 802.11g provides a migration path for 802.11b networks to a frequency compatible standard technology with a higher bit rate. Existing 802.11b wireless network adapters cannot be upgraded to 802.11g by updating the firmware of the adapter, they must be replaced. Unlike migrating from 802.11b to 802.11a (in which all the network adapters in both the wireless clients and the wireless APs must be replaced at the same time), migrating from 802.11b to 802.11g can be done incrementally.

Like 802.11a, 802.11g uses 54 Mbps in ideal conditions and the slower speeds of 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, and 6 Mbps in less than ideal conditions.

802.11n

The IEEE 802.11n standard aims to improve distance (up to 250 m) and network throughput over the two previous standards, 802.11a and 802.11g, with significant increase in the maximum raw data rate from 54 Mbps to 600 Mbps under ideal conditions by adding the multiple-input multiple output technology and channels of 40 MHz, of greater bandwidth. This technology, called MIMO, uses multiple wireless signals and antennas, at the transmitter and receiver. It can be used in the 2.4 GHz or 5 GHz frequency bands.

802.11ac

The 802.11ac standard, an upgrade from 802.11n, provides similar range but increases throughput. It runs on the 5 GHz band and incorporates beam-forming, wide bands and multiple antennas to deliver theoretical data speeds up to 1.3 Gbps, more than double peak rates of 600 Mbps with 802.11n.

5 Security

Wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. However, wireless networks broadcast data in every direction to every device that happens to be listening, within a limited range. A wired network can be secured at its edges, for example, by restricting physical access and installing firewalls. A wireless network with the same measures in place is still vulnerable to eavesdropping. Therefore, wireless networks require a more focused effort to maintain security.

5.1 Secure communications

Communications security is often described in terms of three elements: Authentication, confidentiality and integrity [1].

Authentication ensures that nodes are who and what they claim to be.

Authentication is typically based on demonstrating knowledge of a shared secret, such as a username and password pair. In more complex systems, possession of the shared secret may be demonstrated by proving possession of a token that is more difficult to steal or forge, such as a certificate or a smart card.

Confidentiality ensures that eavesdroppers cannot read network traffic.

Confidentiality is typically protected by encrypting the contents of the message. Encryption applies a known, reversible method of transformation (called a cipher or encryption algorithm) to the original message contents (called the plaintext), scrambling or disguising them to create the ciphertext. Only those who know how to reverse the process (decrypt the message) can recover the original text. The most common forms of encryption are mathematical transformations which use a variable called a key as a part of their manipulations. The intended receiver must know both the correct method and the value of the key that was used, in order to be able to decrypt the message. For commercial encryption schemes, the method will be public knowledge. Protecting the secrecy of the key becomes crucial.

Integrity ensures that messages are delivered without alteration.

In the context of communications security, it refers to the ability to make certain that the message received has not been altered in any way and is identical to the message that was sent. The Frame Check Sequence (FCS) bytes are one example of an integrity check, but they are not considered secure. The ordinary FCS bytes are not calculated over the plaintext message and protected by encryption. Instead they are calculated over the ciphertext, using a known method and sent in the clear (unencrypted). The FCS bytes help to identify packets that have been accidentally damaged in transit. An attacker, however, could recalculate the ordinary FCS (for example, to hide their deliberate alteration of a packet they captured and retransmitted). The harder it is for an attacker to correctly recalculate the integrity check sequence or security hash function, the more reliable a test of message integrity it is.

The concept of integrity is sometimes extended to include verifying that the source of the message is the same as the stated source. Timestamps and message sequence numbers can protect against “replay attacks,” but, again, they are not considered secure unless they are protected by encryption.

Security is always relative, never absolute. For every defense, there is (or will soon be) a successful attack. For every attack, there is (or will soon be) a successful

defense. Only time and effort are really at issue. The better the defense, the more time and effort it takes to breach.

The right defense is the one that is balanced and that matches the expected range of attacks. Balance is important in two senses. First, the weakest link must be secure enough. Second, the passive elements of authentication, encryption, and integrity check must be backed up by active elements such as monitoring and pursuing attempted breaches, maintaining security discipline, and so forth. The right defense is one in which a breach requires just slightly more time and effort from attackers than they are willing to invest. Security measures impose costs and constraints on the defender. Like any other business decision, these trade-offs must be made with eyes open.

5.2 Confidentiality and Encryption

Confidentiality (preventing unauthorized access to message contents) is achieved by protecting the data contents with encryption. Encryption is optional in WLANs, but without it, any similar standards-compliant device within range can read all network traffic.

There have been three major generations of security approaches for WLANs. Since the late 1990s, Wi-Fi security algorithms have undergone multiple upgrades with outright depreciation of older algorithms and significant revision to newer algorithms. In chronological order of introduction, these are:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fi Protected Access)
- WPA2 (Wi-Fi Protected Access, version 2)

WEP

WEP was ratified as a Wi-Fi security standard in September of 1999. The first versions of WEP weren't particularly strong, even for the time they were released, because U.S. restrictions on the export of various cryptographic technologies led to manufacturers restricting their devices to only 64-bit encryption. When the restrictions were lifted, it was increased to 128-bit. Despite the introduction of 256-bit WEP encryption, 128-bit remains one of the most common implementations.

Despite revisions to the algorithm and an increased key size, over time numerous security flaws were discovered in the WEP standard and, as computing power increased, it became easier and easier to exploit them. As early as 2001 proof-of-concept exploits were floating around and by 2005 the FBI gave a public demonstration (in an effort to increase awareness of WEP's weaknesses) where they cracked WEP passwords in minutes using freely available software.

Despite various improvements, work-arounds, and other attempts to shore up the WEP system, it remains highly vulnerable and systems that rely on WEP should be upgraded or, if security upgrades are not an option, replaced. The Wi-Fi Alliance officially retired WEP in 2004.

WPA

To address vulnerabilities in WEP, the Wi-Fi Alliance trade group established WPA at the beginning of 2003. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

Some of the significant changes implemented with WPA included message integrity checks (to determine if an attacker had captured or altered packets passed between the access point and client) and the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key system that was radically more secure than

fixed key used in the WEP system. TKIP was later superseded by Advanced Encryption Standard (AES).

Despite what a significant improvement WPA was over WEP, the ghost of WEP haunted WPA. TKIP, a core component of WPA, was designed to be easily rolled out via firmware upgrades onto existing WEP-enabled devices. As such it had to recycle certain elements used in the WEP system which, ultimately, were also exploited.

WPA, like its predecessor WEP, has been shown via both proof-of-concept and applied public demonstrations to be vulnerable to intrusion. Interestingly the process by which WPA is usually breached is not a direct attack on the WPA algorithm (although such attacks have been successfully demonstrated) but by attacks on a supplementary system that was rolled out with WPA, Wi-Fi Protected Setup (WPS), designed to make it easy to link devices to modern access points.

WPA2

WPA has, as of 2006, been officially superseded by WPA2. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA).

Currently, the primary security vulnerability to the actual WPA2 system is an obscure one (and requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network). As such, the security implications of the known WPA2 vulnerabilities are limited almost entirely to enterprise level networks and deserve little to no practical consideration in regard to home network security.

Unfortunately, the same vulnerability that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points. Although breaking into a WPA/WPA2 secured network using this vulnerability requires anywhere from 2-14 hours of sustained effort with a modern computer, it is still a legitimate security concern and WPS should be disabled (and, if possible, the firmware of the access point should be flashed to a distribution that doesn't even support WPS so the attack vector is entirely removed).

The following is a basic list ranking the current Wi-Fi security methods, ordered from best to worst:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP is there as a fallback method)
4. WPA + TKIP
5. WEP
6. Open Network (no security at all)

Ideally, Wi-Fi Protected Setup (WPS) will be disabled and level of security set to WPA2 +AES. Everything else on the list is a less than ideal step down from that.

6 Advantages and disadvantages

Wireless networks have a number of key benefits over wired networks such as mobility, cost-effectiveness and adaptability, but there are also some disadvantages such as security. Below, main advantages and disadvantages of a wireless network vs wired network are listed.

The following list summarizes some of the benefits of wireless networks:

Increased efficiency

Improved data communications lead to faster transfer of information within businesses and between partners and customers. For example, sales people can remotely check stock levels and prices whilst on sales calls.

Better coverage and mobility

Wires tie you down to one location. Going wireless means you have the freedom to change your location without losing your connection, without the need of extra cables or adaptors to access office networks.

Flexibility

Office-based wireless workers can be networked without sitting at dedicated computers, and can continue to do productive work while away from the office. This can lead to new styles of working, such as home working or direct access to corporate data while on customer sites.

Cost savings

Wireless networks can be easier and cheaper to install, especially in listed buildings or where the landlord will not permit the installation of cables. The absence of wires and cables brings down cost. This is accomplished by a combination of factors, the relatively low cost of wireless routers, no need for trenching, drilling and feeding wires inside the walls or other methods that may be necessary to make physical connections. In addition, no wire maintenance is needed.

Adaptability

Fast and easy integration of devices into the network, and high flexibility when modifying an installation.

New opportunities/applications

Wireless networking could allow you to offer new products or services. For example, many airport departure lounges, train stations, hotels, cafes and restaurants have installed hot spot wireless networking services to allow mobile users to connect their equipment to their home offices while travelling.

There are also certain drawbacks associated with the use of wireless networks.

Security

Wireless transmission is more vulnerable to attack by unauthorized users, so particular attention has to be paid to security.

Installation problems

You may suffer interference if others in the same building also use wireless technology or where other sources of radio signals are present. This could lead to poor communication or, in extreme cases, loss of wireless communication altogether.

Coverage

In some buildings getting consistent coverage can be difficult, leading to black spots where no signal is available. For example, in structures built using steel reinforcing materials, you may find it difficult to pick up the radio frequencies used.

Transmission speeds

Wireless transmission can be slower and less efficient than wired networks. In larger wireless networks the backbone network will usually be wired rather than wireless.

7 Applications

The reach of wireless communication in embedded systems continues to grow. Forrester Research, a company that focuses on the business implications of technology change, has reported that in a few short years, up to 95% of devices used to access the Internet will be non-PC devices that use an embedded system.

There are many applications for embedded devices with a Wi-Fi interface:

- Industrial process and control applications where wired connections are too costly or inconvenient, e.g., continuously moving machinery.
- Emergency applications that require immediate and transitory setup, such as battlefield or disaster situations.
- Mobile applications, such as asset tracking.
- Surveillance cameras (maybe you do not want them easily noticed, cables are difficult to hide).
- Vertical markets like medical, education, and manufacturing.
- Communication with other Wi-Fi devices, like a laptop or a PDA.
- Machine to Machine (M2M) applications.

With reference to the last one, the term Machine to Machine (M2M) refers to technologies that allow both wireless and wired systems to communicate with other devices of the same type. [http://en.wikipedia.org/wiki/Machine_to_machine] Another characteristic of M2M communication is that this interconnection enables primarily automated communication between distant, remote machines and one or more layers of central management applications. It provides for real-time monitoring and control without the need for human intervention.

According to ABI Research, a technology research and advisory corporation, more than 30 billion devices will be wirelessly connected to the Internet of Things (Internet of Everything) by 2020.

In the wireless M2M space, there are two major classes of interconnections: short range and wide area. The predominant wide area technology applies embedded cellular modules to connect remote devices to the internet or application servers. A cellular module includes many of the same features that you would find in a cellular handset, including voice and data communication, and is ideal for embedded applications.

M2M applications are found within a wide range of industries, these include: automatic meter reading (AMR), vending machines, point of sales (POS) terminals, transport and logistics (fleet management), healthcare, security technology and many other applications.

According to ABI Research, a technology research and advisory corporation, more than 30 billion devices will be wirelessly connected to the Internet of Things (Internet of Everything) by 2020.

8 Conclusions

Wireless network technologies connect without wires our high technology devices to either a high speed network or another device. In the past, wires would have to be placed from room to room or floor to floor, price for setup was costly, and the time to setup a wired network was vastly increased from a wireless network among other things.

Nowadays setting up a wireless network setup is really easy to do, and there are a ton of wireless products to choose from in addition to plenty of resources available to help you with setup and configuration of the wireless network if needed.

Different technologies can be chosen to best suit the application requirement and data transmission range can vary from a few meters to several kilometers. Wireless networks certainly offer new opportunities for industrial solutions, but they must be implemented with special attention to security.

Comparison of wireless networks types

Type of network	Name	Standard	Frequency band	Nominal range	Maximum Bit rate
WPAN	Bluetooth	IEEE 802.15.1	2.4 GHz	10 m	720 Kbps
	IrDA	IrDA	Infrared window 850-900 nm wavelength	1 m	16 Mbps
	ZigBee	IEEE 802.15.4	868 MHz, 900 MHz, 2.4 GHz	10 m	250 Kbps
	UWB	IEEE 802.15.3	3.1-10.6 GHz (USA) 3.4-4.8 GHz & 6-8.5 GHz (Europe)	10 m	480 Mbps
WLAN	Wi-Fi	IEEE 802.11	2.4 / 5 GHz	100 m	1 Mbps
		IEEE 802.11a	5 GHz	100 m	48 Mbps
		IEEE 802.11b	2.4 GHz	100 m	11 Mbps
		IEEE 802.11g	2.4 GHz	100 m	54 Mbps
		IEEE 802.11n	2.4 / 5 GHz	250 m	600 Mbps
		IEEE 802.11ac	5 GHz	250 m	1.3 Gbps
WMAN	WiMAX	IEEE 802.16	2-11 GHz and 10-66 GHz	50 km	70 Mbps
WWAN	Cellular	AMPS, GSM, GPRS, UMTS, HSDPA, LTE	700 MHz, 850 MHz, 900 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2600 MHz	> 50 km	1 Gbps
	Satellite	DVB-S2	3-30 GHz	> 50 km	60 Mbps