Recent Advances in Wireless Technologies

Theressa Maddox

First Edition, 2012

ISBN 978-81-323-1057-0

Published by:
College Publishing House
4735/22 Prakashdeep Bldg,
Ansari Road, Darya Ganj,
Delhi - 110002
Email: info@wtbooks.com

Table of Contents

Chapter 1

Wireless Communication

In telecommunications, **wireless communication** is the transfer of information without the use of wires. The distances involved may be short (a few meters as in television remote control) or long (thousands or millions of kilometers for radio communications). The term is often shortened to "wireless". It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of *wireless technology* include GPS units, garage door openers and or garage doors, wireless computer mice, keyboards and headsets, satellite television and cordless telephones.

Introduction

Handheld wireless radios such as this Maritime VHF radio transceiver use electromagnetic waves to implement a form of wireless communications technology.

Wireless operations permits services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls, computer networks, network terminals, etc.)

which use some form of energy (e.g. radio frequency (RF), infrared light, laser light, visible light, acoustic energy, etc.) to transfer information without the use of wires. Information is transferred in this manner over both short and long distances.

Wireless services

The term "wireless" has become a generic and all-encompassing word used to describe communications in which electromagnetic waves or RF (rather than some form of wire) carry a signal over part or the entire communication path. Common examples of wireless equipment in use today include:

- Professional LMR (Land Mobile Radio) and SMR (Specialized Mobile Radio) typically used by business, industrial and Public Safety entities.
- Consumer Two way radio including FRS Family Radio Service, GMRS (General Mobile Radio Service) and Citizens band ("CB") radios.
- The Amateur Radio Service (Ham radio).
- Consumer and professional Marine VHF radios.
- Cellular telephones and pagers: provide connectivity for portable and mobile applications, both personal and business.
- Global Positioning System (GPS): allows drivers of cars and trucks, captains of boats and ships, and pilots of aircraft to ascertain their location anywhere on earth.
- Cordless computer peripherals: the cordless mouse is a common example; keyboards and printers can also be linked to a computer via wireless.
- Cordless telephone sets: these are limited-range devices, not to be confused with cell phones.
- Satellite television: allows viewers in almost any location to select from hundreds of channels.
- Wireless gaming: new gaming consoles allow players to interact and play in the same game regardless of whether they are playing on different consoles. Players can chat, send text messages as well as record sound and send it to their friends. Controllers also use wireless technology. They do not have any cords but they can send the information from what is being pressed on the controller to the main console which then processes this information and makes it happen in the game. All of these steps are completed in milliseconds.

Wireless networks

Wireless networking (i.e. the various types of unlicensed 2.4 GHz WiFi devices) is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location. Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.

Modes

Wireless communication can be via:

- radio frequency communication,
- microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication, or
- infrared (IR) short-range communication, for example from remote controls or via Infrared Data Association (IrDA).

Applications may involve point-to-point communication, point-to-multipoint communication, broadcasting, cellular networks and other wireless networks.

Cordless

The term "wireless" should not be confused with the term "cordless", which is generally used to refer to powered electrical or electronic devices that are able to operate from a portable power source (e.g. a battery pack) without any cable or cord to limit the mobility of the cordless device through a connection to the mains power supply. Some cordless devices, such as cordless telephones, are also wireless in the sense that information is transferred from the cordless telephone to the telephone's base unit via some type of wireless communications link. This has caused some disparity in the usage of the term "cordless", for example in Digital Enhanced Cordless Telecommunications.

History

Early wireless work

David E. Hughes, eight years before Hertz's experiments, transmitted radio signals over a few hundred yards by means of a clockwork keyed transmitter. As this was before Maxwell's work was understood, Hughes' contemporaries dismissed his achievement as mere "Induction". In 1885, T. A. Edison used a vibrator magnet for induction transmission. In 1888, Edison deployed a system of signaling on the Lehigh Valley Railroad. In 1891, Edison obtained the wireless patent for this method using inductance (U.S. Patent 465,971).

In the *history of wireless technology*, the demonstration of the theory of electromagnetic waves by Heinrich Hertz in 1888 was important. The theory of electromagnetic waves

was predicted from the research of James Clerk Maxwell and Michael Faraday. Hertz demonstrated that electromagnetic waves could be transmitted and caused to travel through space at straight lines and that they were able to be received by an experimental apparatus. The experiments were not followed up by Hertz. Jagadish Chandra Bose around this time developed an early wireless detection device and help increase the knowledge of millimeter length electromagnetic waves. Practical applications of wireless radio communication and radio remote control technology were implemented by later inventors, such as Nikola Tesla.

The electromagnetic spectrum

Light, colors, AM and FM radio, and electronic devices make use of the electromagnetic spectrum. In the US, the frequencies that are available for use for communication are treated as a public resource and are regulated by the Federal Communications Commission. This determines which frequency ranges can be used for what purpose and by whom. In the absence of such control or alternative arrangements such as a privatized electromagnetic spectrum, chaos might result if, for example, airlines didn't have specific frequencies to work under and an amateur radio operator were interfering with the pilot's ability to land an airplane. Wireless communication spans the spectrum from 9 kHz to 300 GHz.

Applications of wireless technology

Security systems

Wireless technology may supplement or replace hard wired implementations in security systems for homes or office buildings.

Television remote control

Modern televisions use wireless (generally infrared) remote control units. Now radio waves are also used.

Cellular telephone (phones and modems)

Perhaps the best known example of wireless technology is the cellular telephone and modems. These instruments use radio waves to enable the operator to make phone calls from many locations worldwide. They can be used anywhere that there is a cellular telephone site to house the equipment that is required to transmit and receive the signal that is used to transfer both voice and data to and from these instruments.

Computer interface devices

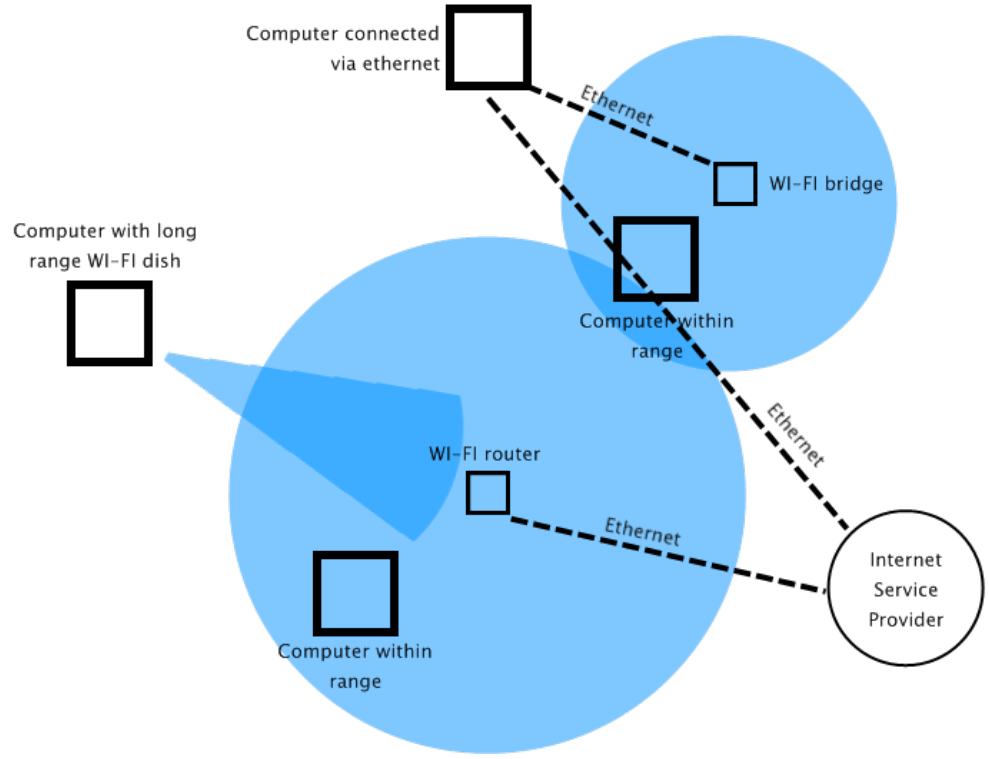
Answering the call of customers frustrated with cord clutter, many manufactures of computer peripherals turned to wireless technology to satisfy their consumer base.

Originally these units used bulky, highly limited transceivers to mediate between a computer and a keyboard and mouse, however more recent generations have used small, high quality devices, some even incorporating Bluetooth. These systems have become so ubiquitous that some users have begun complaining about a lack of wired peripherals. Wireless devices tend to have a slightly slower response time than their wired counterparts, however the gap is decreasing. Initial concerns about the security of wireless keyboards have also been addressed with the maturation of the technology.

Chapter 2

Wireless LAN

The notebook is connected to the wireless access point using a PC card wireless card.

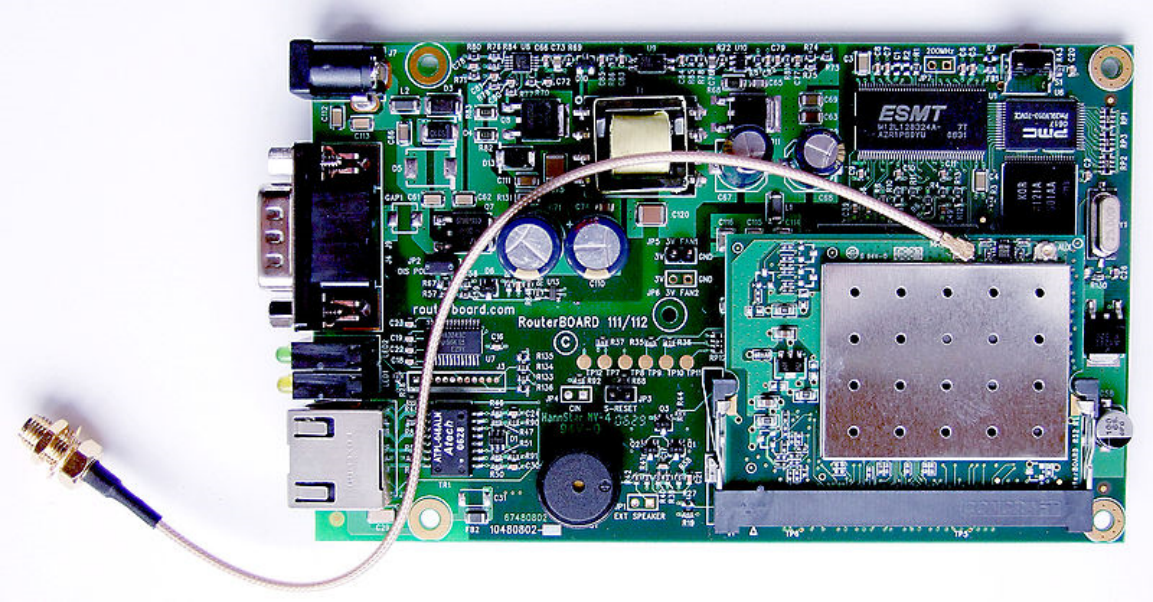


A diagram showing a Wi-Fi network

A **wireless local area network** (**WLAN**) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

Wireless LANs have become popular in the home due to ease of installation, and the increasing popularity of laptop computers. Public businesses such as coffee shops and malls have begun to offer wireless access to their customers; sometimes for free. Large wireless network projects are being put up in many major cities: New York City, for instance, has begun a pilot program to cover all five boroughs of the city with wireless Internet access.

History



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic.

In 1970 Norman Abramson, a professor at the University of Hawaii, developed the world's first wireless computer communication network, ALOHAnet, using low-cost ham-like radios. The bi-directional star topology of the system included seven computers were deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines.

"In 1979, F.R. Gfeller and U. Bapst published a paper in the IEEE Proceedings reporting an experimental wireless local area network using diffused infrared communications. Shortly thereafter, in 1980, P. Ferrert reported on an experimental application of a single code spread spectrum radio for wireless terminal communications in the IEEE National Telecommunications Conference. In 1984, a comparison between infrared and CDMA spread spectrum communications for wireless office information networks was published by Kaveh Pahlavan in IEEE Computer Networking Symposium which appeared later in the IEEE Communication Society Magazine. In May 1985, the efforts of Marcus led the FCC to announce experimental ISM bands for commercial application of spread spectrum technology. Later on, M. Kavehrad reported on an experimental wireless PBX system using code division multiple access. These efforts prompted significant industrial activities in the development of a new generation of wireless local area networks and it updated several old discussions in the portable and mobile radio industry.

The first generation of wireless data modems was developed in the early 1980s by amateur radio operators, who commonly referred to this as packet radio. They added a voice band data communication modem, with data rates below 9600-bit/s, to an existing short distance radio system, typically in the two meter amateur band. The second

generation of wireless modems was developed immediately after the FCC announcement in the experimental bands for non-military use of the spread spectrum technology. These modems provided data rates on the order of hundreds of kbit/s. The third generation of wireless modem then aimed at compatibility with the existing LANs with data rates on the order of Mbit/s. Several companies developed the third generation products with data rates above 1 Mbit/s and a couple of products had already been announced by the time of the first IEEE Workshop on Wireless LANs."

54 MBit/s WLAN PCI Card (802.11g)

"The first of the IEEE Workshops on Wireless LAN was held in 1991. At that time early wireless LAN products had just appeared in the market and the IEEE 802.11 committee had just started its activities to develop a standard for wireless LANs. The focus of that first workshop was evaluation of the alternative technologies. By 1996, the technology was relatively mature, a variety of applications had been identified and addressed and technologies that enable these applications were well understood. Chip sets aimed at wireless LAN implementations and applications, a key enabling technology for rapid market growth, were emerging in the market. Wireless LANs were being used in hospitals, stock exchanges, and other in building and campus settings for nomadic access, point-to-point LAN bridges, ad-hoc networking, and even larger applications through internetworking. The IEEE 802.11 standard and variants and alternatives, such as the wireless LAN interoperability forum and the European HiperLAN specification had made

rapid progress, and the unlicensed PCS Unlicensed Personal Communications Services and the proposed SUPERNet, later on renamed as U-NII, bands also presented new opportunities."

WLAN hardware was initially so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802.11 (Wi-Fi). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802.11a (5 GHz) and 802.11g (2.4 GHz) standards, almost certainly never will.

Architecture

Stations

All components that can connect into a wireless medium in a network are referred to as stations.

All stations are equipped with wireless network interface cards (WNICs).

Wireless stations fall into one of two categories: access points, and clients.

Access points (APs), normally routers, are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with.

Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface.

Basic service set

The basic service set (BSS) is a set of all stations that can communicate with each other.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS.

Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS.

An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they can not connect to any other basic service set.

An infrastructure can communicate with other stations not in the same basic service set by communicating through access points.

Extended service set

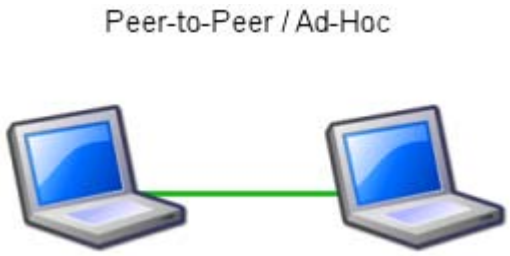
An extended service set (ESS) is a set of connected BSSes. Access points in an ESS are connected by a distribution system. Each ESS has an ID called the SSID which is a 32-byte (maximum) character string.

Distribution system

A distribution system (DS) connects access points in an extended service set. The concept of a DS can be used to increase network coverage through roaming between cells.

Types of wireless LANs

Peer-to-peer

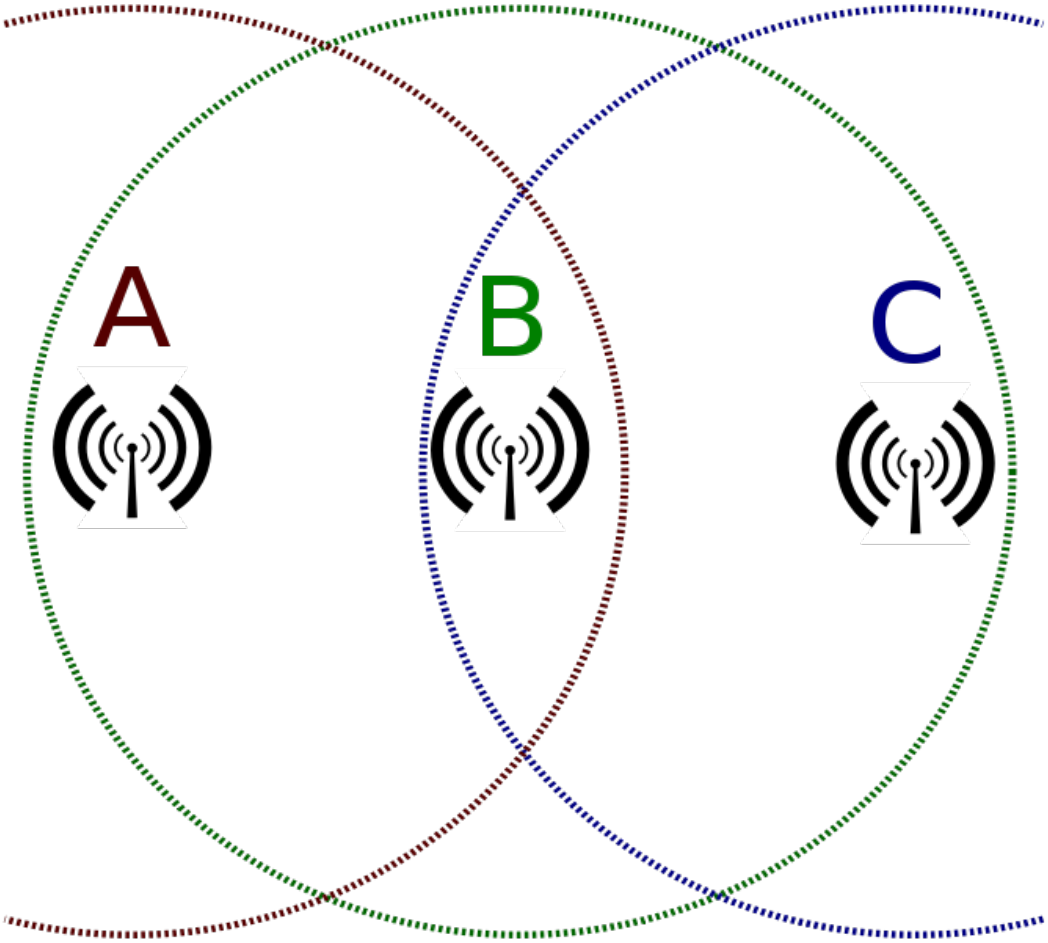


Peer-to-Peer or ad-hoc wireless LAN

An ad-hoc network is a network where stations communicate only peer to peer (P2P). There is no base and no one gives permission to talk. This is accomplished using the Independent Basic Service Set (IBSS).

A peer-to-peer (P2P) network allows wireless devices to directly communicate with each other. Wireless devices within range of each other can discover and communicate directly without involving central access points. This method is typically used by two computers so that they can connect to each other to form a network.

If a signal strength meter is used in this situation, it may not read the strength accurately and can be misleading, because it registers the strength of the strongest signal, which may be the closest computer.



Hidden node problem: Devices A and C are both communicating with B, but are unaware of each other

IEEE 802.11 define the physical layer (PHY) and MAC (Media Access Control) layers based on CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). The 802.11 specification includes provisions designed to minimize collisions, because two mobile units may both be in range of a common access point, but out of range of each other.

The 802.11 has two basic modes of operation: Ad hoc mode enables peer-to-peer transmission between mobile units. Infrastructure mode in which mobile units communicate through an access point that serves as a bridge to a wired network infrastructure is the more common wireless LAN application the one being covered. Since wireless communication uses a more open medium for communication in comparison to wired LANs, the 802.11 designers also included shared-key encryption mechanisms: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA, WPA2), to secure wireless computer networks.

Bridge

A bridge can be used to connect networks, typically of different types. A wireless Ethernet bridge allows the connection of devices on a wired Ethernet network to a wireless network. The bridge acts as the connection point to the Wireless LAN.

Wireless distribution system

A Wireless Distribution System is a system that enables the wireless interconnection of access points in an IEEE 802.11 network. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required. The notable advantage of WDS over other solutions is that it preserves the MAC addresses of client packets across links between access points.

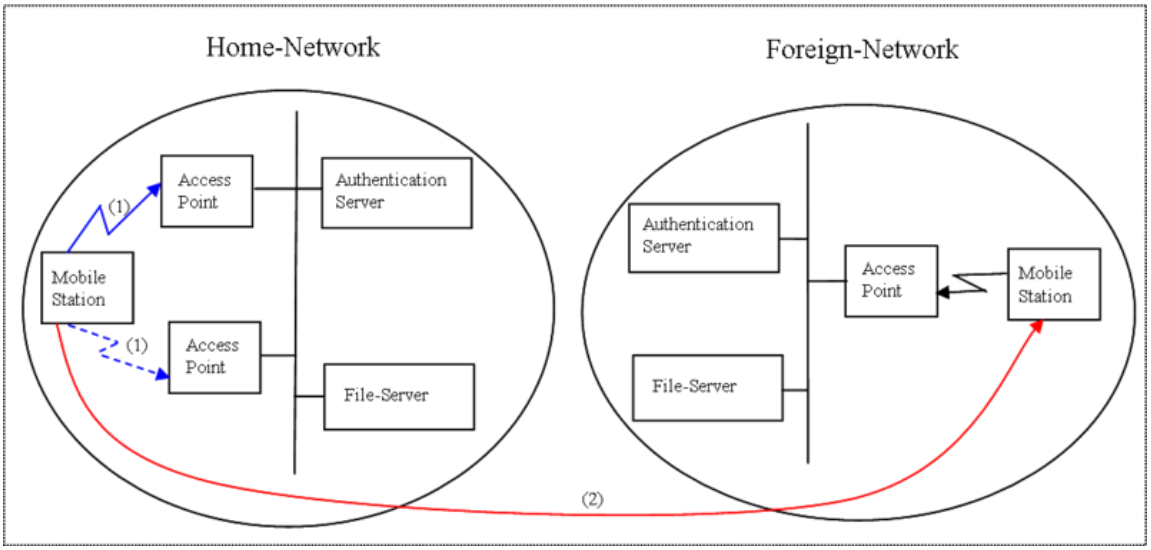
An access point can be either a main, relay or remote base station. A main base station is typically connected to the wired Ethernet. A relay base station relays data between remote base stations, wireless clients or other relay stations to either a main or another relay base station. A remote base station accepts connections from wireless clients and passes them to relay or main stations. Connections between "clients" are made using MAC addresses rather than by specifying IP assignments.

All base stations in a Wireless Distribution System must be configured to use the same radio channel, and share WEP keys or WPA keys if they are used. They can be configured to different service set identifiers. WDS also requires that every base station be configured to forward to others in the system.

WDS may also be referred to as repeater mode because it appears to bridge and accept wireless clients at the same time (unlike traditional bridging). It should be noted, however, that throughput in this method is halved for all clients connected wirelessly.

When it is difficult to connect all of the access points in a network by wires, it is also possible to put up access points as repeaters.

Roaming



Roaming between Wireless Local Area Networks

There are 2 definitions for wireless LAN roaming:

- Internal Roaming (1): The Mobile Station (MS) moves from one access point (AP) to another AP within a home network because the signal strength is too weak. An authentication server (RADIUS) assumes the re-authentication of MS via 802.1x (e.g. with PEAP). The billing of QoS is in the home network. A Mobile Station roaming from one access point to another often interrupts the flow of data between the Mobile Station and an application connected to the network. The Mobile Station, for instance, periodically monitors the presence of alternative access points (ones that will provide a better connection). At some point, based upon proprietary mechanisms, the Mobile Station decides to re-associate with an access point having a stronger wireless signal. The Mobile Station, however, may lose a connection with an access point before associating with another access point. In order to provide reliable connections with applications, the Mobile Station must generally include software that provides session persistence.

- External Roaming (2): The MS(client) moves into a WLAN of another Wireless Internet Service Provider (WISP) and takes their services (Hotspot). The user can independently of his home network use another foreign network, if this is open for visitors. There must be special authentication and billing systems for mobile services in a foreign network.

Wireless LAN security

One issue with corporate wireless networks in general, and WLANs in particular, involves the need for security. Many early access points could not discern whether or not a particular user had authorization to access the network. Although this problem reflects issues that have long troubled many types of wired networks (it has been possible in the past for individuals to plug computers into randomly available Ethernet jacks and get access to a local network), this did not usually pose a significant problem, since many organizations had reasonably good physical security. However, the fact that radio signals bleed outside of buildings and across property lines makes physical security largely irrelevant to Piggybackers. Such corporate issues are covered in wireless security.

Concerns

Anyone within the geographical network range of an open, unencrypted wireless network can 'sniff' or record the traffic, gain unauthorized access to internal network resources as well as to the internet, and then possibly send spam or do other illegal actions using the wireless network's IP address, all of which are rare for home routers but may be significant concerns for office networks.

If router security is not activated or if the owner deactivates it for convenience, it creates a free hotspot. Since most 21st century laptop PCs have wireless networking built in (cf. Intel 'Centrino' technology), they don't need a third-party adapter such as a PCMCIA Card or USB dongle. Built in wireless networking might be enabled by default, without the owner realizing it, thus broadcasting the laptop's accessibility to any computer nearby.

Modern operating systems such as Mac OS, or Microsoft Windows make it fairly easy to set up a PC as a wireless LAN 'base station' using Internet Connection Sharing, thus allowing all the PCs in the home to access the Internet via the 'base' PC. However, lack of knowledge about the security issues in setting up such systems often means that someone nearby may also use the connection. Such "piggybacking" is usually achieved without the wireless network operators knowledge; it may even be without the knowledge of the intruding user if their computer automatically selects a nearby unsecured wireless network to use as an access point.

Security options

There are three principal ways to secure a wireless network.

- For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address. Another option is to disable ESSID broadcasting, making the access point difficult for outsiders to detect.

Wireless Intrusion Prevention Systems can be used to provide wireless LAN security in this network model.

- For commercial providers, hotspots, and large organizations, the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN.
- Wireless networks are less secure than wired ones; in many offices intruders can easily visit and hook up their own computer to the wired network without problems, gaining access to the network, and it's also often possible for remote intruders to gain access to the network through backdoors like Back Orifice. One general solution may be end-to-end encryption, with independent authentication on all resources that shouldn't be available to the public.

Access Control at the Access Point level

One of the simplest techniques is to only allow access from known, approved MAC addresses. However, this approach gives no security against sniffing, and client devices can easily spoof MAC addresses, leading to the need for more advanced security measures.

Some access points can also support "AP isolation" which isolates all wireless clients and wireless devices on the network from each other. Wireless devices will be able to communicate with the gateway but not with each other in the network.

Another very simple technique is to have a secret ESSID (id/name of the wireless network), though anyone who studies the method will be able to sniff the ESSID.

Today all (or almost all) access points incorporate Wired Equivalent Privacy (WEP) encryption and most wireless routers are sold with WEP turned on. However, security analysts have criticized WEP's inadequacies, and the U.S. FBI has demonstrated the ability to break WEP protection in only three minutes using tools available to the general public.

The Wi-Fi Protected Access (WPA and WPA2) security protocols were later created to address these problems. If a weak password, such as a dictionary word or short character string is used, WPA and WPA2 can be cracked. Using a long enough random password (e.g. 14 random letters) or passphrase (e.g. 5 randomly chosen words) makes pre-shared key WPA virtually uncrackable. The second generation of the WPA security protocol (WPA2) is based on the final IEEE 802.11i amendment to the 802.11 standard and is eligible for FIPS 140-2 compliance. With all those encryption schemes, any client in the network that knows the keys can read all the traffic.

Restricted access networks

Solutions include a newer system for authentication, IEEE 802.1x, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

End-to-End encryption

One can argue that both layer 2 and layer 3 encryption methods are not good enough for protecting valuable data like passwords and personal emails. Those technologies add encryption only to parts of the communication path, still allowing people to spy on the traffic if they have gained access to the wired network somehow. The solution may be encryption and authorization in the application layer, using technologies like SSL, SSH, GnuPG, PGP and similar.

The disadvantage with the end to end method is, it may fail to cover all traffic. With encryption on the router level or VPN, a single switch encrypts all traffic, even UDP and DNS lookups. With end-to-end encryption on the other hand, each service to be secured must have its encryption "turned on," and often every connection must also be "turned on" separately. For sending emails, every recipient must support the encryption method, and must exchange keys correctly. For Web, not all web sites offer https, and even if they do, the browser sends out IP addresses in clear text.

The most prized resource is often access to Internet. An office LAN owner seeking to restrict such access will face the non trivial enforcement task of having each user authenticate himself for the router.

Open Access Points

Today, there is almost full wireless network coverage in many urban areas - the infrastructure for the wireless community network (which some consider to be the future of the internet) is already in place. One could roam around and always be connected to Internet if the nodes were open to the public, but due to security concerns, most nodes are encrypted and the users don't know how to disable encryption. Many people consider it proper etiquette to leave access points open to the public, allowing free access to Internet. Others think the default encryption provides substantial protection at small inconvenience, against dangers of open access that they fear may be substantial even on a home DSL router.

The density of access points can even be a problem - there are a limited number of channels available, and they partly overlap. Each channel can handle multiple networks, but places with many private wireless networks (for example, apartment complexes), the limited number of Wi-Fi radio channels might cause slowness and other problems.

According to the advocates of Open Access Points, it shouldn't involve any significant risks to open up wireless networks for the public:

- The wireless network is after all confined to a small geographical area. A computer connected to the Internet and having improper configurations or other security problems can be exploited by anyone from anywhere in the world, while only clients in a small geographical range can exploit an open wireless access point. Thus the exposure is low with an open wireless access point, and the risks with having an open wireless network are small. However, one should be aware that an open wireless router will give access to the local network, often including access to file shares and printers.
- The only way to keep communication truly secure is to use end-to-end encryption. For example, when accessing an internet bank, one would almost always use strong encryption from the web browser and all the way to the bank - thus it shouldn't be risky to do banking over an unencrypted wireless network. The argument is that anyone can sniff the traffic applies to wired networks too, where system administrators and possible crackers have access to the links and can read the traffic. Also, anyone knowing the keys for an encrypted wireless network can gain access to the data being transferred over the network.
- If services like file shares, access to printers etc. are available on the local net, it is advisable to have authentication (i.e. by password) for accessing it (one should never assume that the private network is not accessible from the outside). Correctly set up, it should be safe to allow access to the local network to outsiders.
- With the most popular encryption algorithms today, a sniffer will usually be able to compute the network key in a few minutes.
- It is very common to pay a fixed monthly fee for the Internet connection, and not for the traffic - thus extra traffic will not hurt.
- Where Internet connections are plentiful and cheap, freeloaders will seldom be a prominent nuisance.

On the other hand, in some countries including Germany, persons providing an open access point may be made (partially) liable for any illegal activity conducted via this access point.

Chapter 3

Wireless Wide Area Network

WWAN, which stands for *Wireless wide area network*, is a form of wireless network. A wide area network differs from a local area network by the technology used to transmit the signal and their size. Wireless networks of all sizes deliver data in the form of telephone calls, web pages, and streaming video.

Description

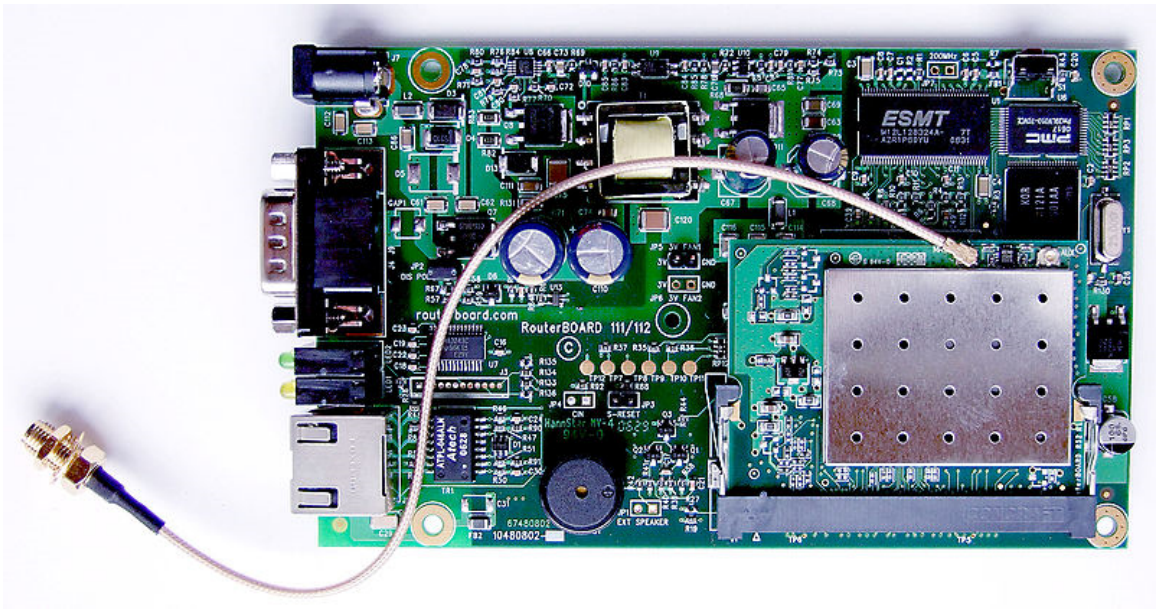
A WWAN differs from WLAN (wireless LAN) in that it uses mobile telecommunication cellular network technologies such as WIMAX (though it's better applied to WMAN Networks), UMTS, GPRS, EDGE, CDMA2000, GSM, CDPD, Mobitex, HSDPA, HSUPA or 3G to transfer data. It can also use LMDS and Wi-Fi to connect to the internet. These cellular technologies are offered regionally, nationwide, or even globally and are provided by a wireless service provider. WWAN connectivity allows a user with a laptop and a WWAN card to surf the web, check email, or connect to a virtual private network (VPN) from anywhere within the regional boundaries of cellular service. Various computers now have integrated WWAN capabilities (such as HSDPA in Centrino). This means that the system has a cellular radio (GSM/CDMA) built in, which allows the user to send and receive data.

Since radio communications systems do not provide a physically secure connection path, WWANs typically incorporate encryption and authentication methods to make them more secure. Unfortunately some of the early GSM encryption techniques were flawed, and security experts have issued warnings that cellular communication, including WWAN, is no longer secure. UMTS (3G) encryption was developed later and has yet to be broken.

Examples of providers for WWAN include T-Mobile, Sprint Nextel, Verizon, and AT&T.

Wireless Internet service provider

Aspen Communication's wireless access point in Tyler, Texas



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 miniPCI Wi-Fi card widely used by WISPs in the Czech Republic

Typical WISP Customer-premises equipment (CPE) installed on a residence.

Wireless Internet Service Providers (**WISPs**) are Internet service providers with networks built around wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900MHz, 2.4GHz, 4.9, 5.2, 5.4, 5.7, and 5.8GHz bands or licensed frequencies in the UHF or MMDS bands.

In the US, the Federal Communications Commission (FCC) released Report and Order, FCC 05-56 in 2005 that revised the FCC's rules to open the 3650 MHz band for terrestrial wireless broadband operations. On November 14, 2007 the Commission released Public Notice (DA 07-4605) in which the Wireless Telecommunications Bureau announced the start date for licensing and registration process for the 3650-3700 MHz band.

History

Initially, WISPs were only found in rural areas not covered by cable or DSL. The first WISP in the world was LARIAT, a non-profit rural telecommunications cooperative founded in 1992 by Brett Glass in Laramie, Wyoming. LARIAT originally used WaveLAN equipment, manufactured by the NCR Corporation, which operated on the 900MHz unlicensed radio band. LARIAT was taken private in 2003 and continues to exist as a for-profit wireless ISP.

Another early WISP was a company called Internet Office Parks in Johannesburg, South Africa that was founded by Roy Pater, Brett Airey and Attila Barath in January 1996 when they realized the South African Telco, Telkom could not keep up with the demand for dedicated Internet links for business use. Using what was one of the first wireless LAN products available for wireless barcode scanning in stores, called Aironet (now owned by Cisco), they worked out if they ran a dedicated Telco link into the highest building in a business area or CBD they could wirelessly "cable" up all the other buildings back to this main point and would only require one link from the Telco to connect up hundreds of businesses at the same time. In turn each "satellite" building was wired up with Ethernet so each business connected into the Ethernet LAN and could instantly get Internet access. Due to the immaturity of wireless technology, security issues and being forced constantly by Telkom SA (The government Telco in South Africa) to cease its service, the company closed its doors in Jan 1999.

There were 879 Wi-Fi based WISPs in the Czech Republic as of May 2008, making it the country with most Wi-Fi access points in the whole EU. The providing of wireless Internet has a big potential of lowering the "digital gap" or "Internet gap" in the developing countries. Geekcorps actively help in Africa with among others wireless network building. An example of a typical WISP system is such as the one deployed by Gaiacom Wireless Networks which is based on WiFi standards. The OLPC project strongly relies on good Internet connectivity, which can most likely be provided in rural areas only with satellite or wireless network Internet access.

Overview

WISPs often offer additional services like location based content, Virtual Private Networking and Voice over IP. Isolated municipal ISPs and larger state-wide initiatives alike are tightly focused on wireless networking.

WISPs are predominantly in rural environments where cable and digital subscriber lines are not available. WiMax is expected to become mainstream in the near future, bringing with it dramatic changes to the marketplace by increasing the number of interoperable equipment on the market and making mobile data transmission feasible, increasing the utility of such networks in rural environments. However, high-bandwidth wireless backhauls are already common in major cities, providing levels of bandwidth previously only available through expensive fiber optic connections.

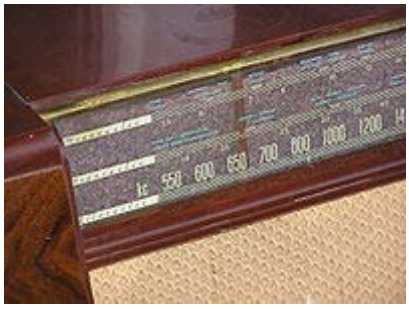
Typically, the way that a WISP operates is to pull a large and usually expensive point to point connection to the center of the area they wish to service. From here, they will need to find some sort of elevated point in the region, such as a radio or water tower, on which to mount their equipment. The WISP may also connect to a PoP (Point of Presence) and then backhaul to their towers, reducing the need to pull a point to point connection to the tower. On the consumers side, they will mount a small dish or antenna to the roof of their home and point it back to the WISP's nearest antenna site. When operating over the tightly limited range of the heavily populated 2.4 GHz band, as nearly all 802.11-based WiFi providers do, it is not uncommon to also see access points mounted on light posts and customer buildings.

Since it is difficult for a single service provider to build an infrastructure that offers global access to its subscribers, roaming between service providers is encouraged by the Wi-Fi Alliance with the *WISPr* protocol. WISPr is a set of recommendations approved by the alliance which facilitate inter-network and inter-operator roaming of Wi-Fi users. Modern wireless services have comparable latency to other terrestrial broadband networks.

Chapter 4

Radio

Radio



Classic radio receiver dial

Radio is the transmission of signals by modulation of electromagnetic waves with frequencies below those of visible light. Electromagnetic radiation travels by means of oscillating electromagnetic fields that pass through the air and the vacuum of space. Information is carried by systematically changing (modulating) some property of the radiated waves, such as amplitude, frequency, phase, or pulse width. When radio waves pass an electrical conductor, the oscillating fields induce an alternating current in the conductor. This can be detected and transformed into sound or other signals that carry information.

Etymology

The etymology of "radio" or "radiotelegraphy" reveals that it was called "wireless telegraphy", which was shortened to "wireless" in Britain. The prefix *radio-* in the sense of wireless transmission, was first recorded in the word *radioconductor*, a description provided by the French physicist Édouard Branly in 1897. It is based on the verb *to radiate* (in Latin "radius" means "spoke of a wheel, beam of light, ray"). This word also appears in a 1907 article by Lee De Forest, it was adopted by the United States Navy in 1912, and became common by the time of the first commercial broadcasts in the United States in the 1920s. (The noun "broadcasting" itself came from an agricultural term, meaning "scattering seeds widely".) The term was then adopted by other languages in Europe and Asia. British Commonwealth countries continued to mainly use the term

"wireless" until the mid-20th century, though the magazine of the BBC in the UK has been called Radio Times ever since it was first published in the early 1920s.

In recent years the term "wireless" has gained renewed popularity through the rapid growth of short-range computer networking, e.g., Wireless Local Area Network (WLAN), Wi-Fi, and Bluetooth, as well as mobile telephony, e.g., GSM and UMTS. Today, the term "radio" often refers to the actual transceiver device or chip, whereas "wireless" refers to the system and/or method used for radio communication; hence one talks about *radio* transceivers and *Radio* Frequency Identification (RFID), but about *wireless* devices and *wireless* sensor networks.

Processes

Radio systems used for communications will have the following elements. With more than 100 years of development, each process is implemented by a wide range of methods, specialized for different communications purposes.

Each system contains a transmitter. This consists of a source of electrical energy, producing alternating current of a desired frequency of oscillation. The transmitter contains a system to modulate (change) some property of the energy produced to impress a signal on it. This modulation might be as simple as turning the energy on and off, or altering more subtle properties such as amplitude, frequency, phase, or combinations of these properties. The transmitter sends the modulated electrical energy to a tuned resonant antenna; this structure converts the rapidly changing alternating current into an electromagnetic wave that can move through free space (sometimes with a particular polarization).

Electromagnetic waves travel through space either directly, or have their path altered by reflection, refraction or diffraction. The intensity of the waves diminishes due to geometric dispersion (the inverse-square law); some energy may also be absorbed by the intervening medium in some cases. Noise will generally alter the desired signal; this electromagnetic interference comes from natural sources, as well as from artificial sources such as other transmitters and accidental radiators. Noise is also produced at every step due to the inherent properties of the devices used. If the magnitude of the noise is large enough, the desired signal will no longer be discernible; this is the fundamental limit to the range of radio communications.

The electromagnetic wave is intercepted by a tuned receiving antenna; this structure captures some of the energy of the wave and returns it to the form of oscillating electrical currents. At the receiver, these currents are demodulated, which is conversion to a usable signal form by a detector sub-system. The receiver is "tuned" to respond preferentially to the desired signals, and reject undesired signals.

Early radio systems relied entirely on the energy collected by an antenna to produce signals for the operator. Radio became more useful after the invention of electronic devices such as the vacuum tube and later the transistor, which made it possible to

amplify weak signals. Today radio systems are used for applications from walkie-talkie children's toys to the control of space vehicles, as well as for broadcasting, and many other applications.

Electromagnetic spectrum

Radio frequencies occupy the range from a few tens of hertz to three hundred gigahertz, although commercially important uses of radio use only a small part of this spectrum. Other types of electromagnetic radiation, with frequencies above the RF range, are microwave, infrared, visible light, ultraviolet, X-rays and gamma rays. Since the energy of an individual photon of radio frequency is too low to remove an electron from an atom, radio waves are classified as non-ionizing radiation.

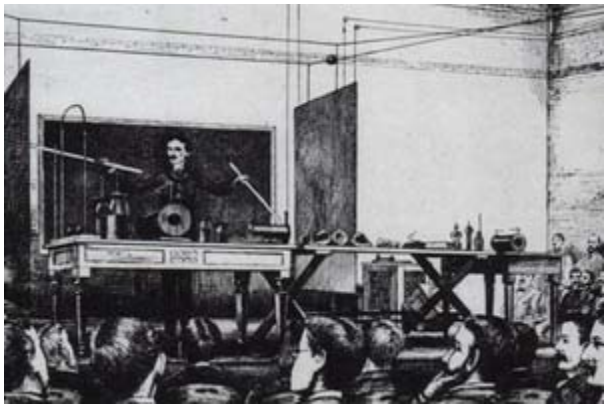
History

19th century

The meaning and usage of the word "radio" has developed in parallel with developments within the field of communications and can be seen to have three distinct phases: electromagnetic waves and experimentation; wireless communication and technical development; and radio broadcasting and commercialization. Many individuals—inventors, engineers, developers, businessmen - contributed to produce the modern idea of radio and thus the origins and 'invention' are multiple and controversial. Early radio designs could not transmit sound or speech and were called the "wireless telegraph".

Development from a laboratory demonstration to a commercial entity spanned several decades and required the efforts of many practitioners. In 1878, David E. Hughes noticed that sparks could be heard in a telephone receiver when experimenting with his carbon microphone. He developed this carbon-based detector further and eventually could detect signals over a few hundred yards. He demonstrated his discovery to the Royal Society in 1880, but was told it was merely induction, and therefore abandoned further research.

Experiments, later patented, were undertaken by Thomas Edison and his employees of Menlo Park. Edison applied in 1885 to the U.S. Patent Office for his patent on an electrostatic coupling system between elevated terminals. The patent was granted as U.S. Patent 465,971 on December 29, 1891. The Marconi Company would later purchase rights to the Edison patent to protect them legally from lawsuits.



Tesla demonstrating wireless transmissions during his high frequency and potential lecture of 1891. After continued research, Tesla presented the fundamentals of radio in 1893.

In 1893, in St. Louis, Missouri, Nikola Tesla made devices for his experiments with electricity. Addressing the *Franklin Institute* in Philadelphia and the *National Electric Light Association*, he described and demonstrated the principles of his wireless work. The descriptions contained all the elements that were later incorporated into radio systems before the development of the vacuum tube. He initially experimented with magnetic receivers, unlike the coherers (detecting devices consisting of tubes filled with iron filings which had been invented by Temistocle Calzecchi-Onesti at Fermo in Italy in 1884) used by Guglielmo Marconi and other early experimenters.

A demonstration of wireless telegraphy took place in the lecture theater of the Oxford University Museum of Natural History on August 14, 1894, carried out by Professor Oliver Lodge and Alexander Muirhead. During the demonstration a radio signal was sent from the neighboring Clarendon laboratory building, and received by apparatus in the lecture theater.

In 1895 Alexander Stepanovich Popov built his first radio receiver, which contained a coherer. Further refined as a lightning detector, it was presented to the Russian Physical and Chemical Society on May 7, 1895. A depiction of Popov's lightning detector was printed in the Journal of the Russian Physical and Chemical Society the same year. Popov's receiver was created on the improved basis of Lodge's receiver, and originally intended for reproduction of its experiments.

In 1895, Marconi built a wireless system capable of transmitting signals at long distances (1.5 mi./ 2.4 km). In radio transmission technology, early public experimenters had made short distance broadcasts. Marconi achieved long range signalling due to a wireless transmitting apparatus and a radio receiver claimed by him. From Marconi's experiments, the phenomenon that transmission range is proportional to the square of antenna height is known as "Marconi's law". This formula represents a physical law that radio devices use. Marconi's experimental apparatus proved to be a complete, commercially successful radio transmission system. According to the *Proceedings of the United States Naval Institute* in 1899, the Marconi instruments had a "[...] coherer, principle of which was

discovered some twenty years ago, [and was] the only electrical instrument or device contained in the apparatus that is at all new".

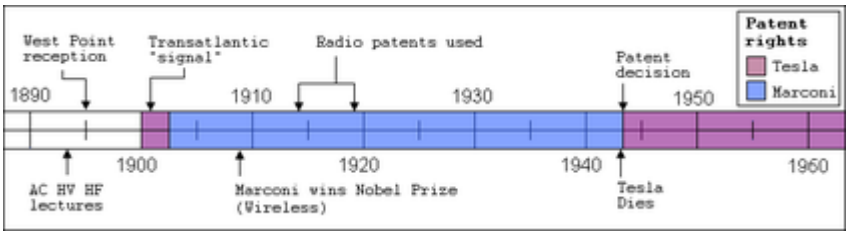
Telephone Herald in Budapest, Hungary (1901).

In 1896, Marconi was awarded British patent 12039, *Improvements in transmitting electrical impulses and signals and in apparatus there-for*, for radio. In 1897, he established a radio station on the Isle of Wight, England. Marconi opened his "wireless" factory in Hall Street, Chelmsford, England in 1898, employing around 50 people. Shortly after the 1900s, Marconi held the patent rights for radio.

20th century

The next advancement was the vacuum tube detector, invented by Westinghouse engineers. On Christmas Eve, 1906, Reginald Fessenden used a synchronous rotary-spark transmitter for the first radio program broadcast, from Ocean Bluff-Brant Rock, Massachusetts. Ships at sea heard a broadcast that included Fessenden playing *O Holy Night* on the violin and reading a passage from the Bible. This was, for all intents and purposes, the first transmission of what is now known as amplitude modulation or AM radio. The first radio news program was broadcast August 31, 1920 by station 8MK in Detroit, Michigan, which survives today as all-news format station WWJ under ownership of the CBS network. The first college radio station began broadcasting on October 14, 1920, from Union College, Schenectady, New York under the personal call letters of Wendell King, an African-American student at the school. That month 2ADD, later renamed WRUC in 1947, aired what is believed to be the first public entertainment broadcast in the United States, a series of Thursday night concerts initially heard within a 100-mile (160 km) radius and later for a 1,000-mile (1,600 km) radius. In November 1920, it aired the first broadcast of a sporting event. At 9 pm on August 27, 1920, Sociedad Radio Argentina aired a live performance of Richard Wagner's Parsifal opera from the Coliseo Theater in downtown Buenos Aires. Only about twenty homes in the city had receivers to tune in this radio program. Meanwhile, regular entertainment broadcasts commenced in 1922 from the Marconi Research Centre at Writtle, England.

Sports broadcasting began at this time as well, including the first broadcast college football game.



Patent rights after the 1900s.

In 1943 the United States Supreme Court upheld Tesla's patent for radio, number 645,576 (1897), with the supreme court's justification that claim 16 in Marconi's related patent, number 763,772 (1904), contained nothing new not having been published earlier and registered by Tesla, Lodge, and others. After years of patent battles by Marconi's company, the United States Supreme Court, in the 1943 case "Marconi Wireless Telegraph co. of America v. United States", held regarding the priority of engineering advances concerning the invention of radio that "[but] it is now held that in the important advance upon his basic patent Marconi did nothing that had not already been seen and disclosed". The decision effectively awarded priority of the invention of radio to Tesla and his 1893 presentation in St. Louis. Although Marconi claimed that he had no knowledge of prior art taken from Tesla's patents, the supreme court considered his claim false. In addition to the June 21, 1943 ruling made by the supreme court, the United States Court of Claims also invalidated the fundamental Marconi patent earlier, in 1935. This case defined radio by the statement: "A radio communication system requires two tuned circuits each at the transmitter and receiver, all four tuned to the same frequency." Because Tesla's 1897 patent for radio was intended for general transmission of energy, the court determined that Tesla's patent clearly was the first to disclose a system which could be used for wireless communication of intelligible messages (such as human voice and music) and used the four-circuit tuned combination.

American girl listens to radio during the Great Depression.

One of the first developments in the early 20th century was that aircraft used commercial AM radio stations for navigation. This continued until the early 1960s when VOR systems became widespread. In the early 1930s, single sideband and frequency modulation were invented by amateur radio operators. By the end of the decade, they were established commercial modes. Radio was used to transmit pictures visible as television as early as the 1920s. Commercial television transmissions started in North America and Europe in the 1940s.

In 1954, the Regency company introduced a pocket transistor radio, the TR-1, powered by a "standard 22.5 V Battery". In 1955, the newly formed Sony company introduced its first transistorized radio. It was small enough to fit in a vest pocket, and able to be powered by a small battery. It was durable, because it had no vacuum tubes to burn out. Over the next 20 years, transistors replaced tubes almost completely except for very high-power transmitter uses. By 1963, color television was being regularly broadcast commercially (though not all broadcasts or programs were in color), and the first (radio) communication satellite, *Telstar*, was launched. In the late 1960s, the U.S. long-distance telephone network began to convert to a digital network, employing digital radios for many of its links. In the 1970s, LORAN became the premier radio navigation system. Soon, the U.S. Navy experimented with satellite navigation, culminating in the invention and launch of the GPS constellation in 1987. In the early 1990s, amateur radio experimenters began to use personal computers with audio cards to process radio signals. In 1994, the U.S. Army and DARPA launched an aggressive, successful project to construct a software-defined radio that can be programmed to be virtually any radio by changing its software program. Digital transmissions began to be applied to broadcasting in the late 1990s.

Uses of radio

Early uses were maritime, for sending telegraphic messages using Morse code between ships and land. The earliest users included the Japanese Navy scouting the Russian fleet during the Battle of Tsushima in 1905. One of the most memorable uses of marine telegraphy was during the sinking of the RMS *Titanic* in 1912, including communications between operators on the sinking ship and nearby vessels, and communications to shore stations listing the survivors.

Radio was used to pass on orders and communications between armies and navies on both sides in World War I; Germany used radio communications for diplomatic messages once it discovered that its submarine cables had been tapped by the British. The United States passed on President Woodrow Wilson's Fourteen Points to Germany via radio during the war. Broadcasting began from San Jose, California in 1909, and became feasible in the 1920s, with the widespread introduction of radio receivers, particularly in Europe and the United States. Besides broadcasting, point-to-point broadcasting, including telephone messages and relays of radio programs, became widespread in the 1920s and 1930s. Another use of radio in the pre-war years was the development of detection and locating of aircraft and ships by the use of radar (*RA*dio *D*etection *A*nd *R*anging).

Today, radio takes many forms, including wireless networks and mobile communications of all types, as well as radio broadcasting. Before the advent of television, commercial radio broadcasts included not only news and music, but dramas, comedies, variety shows, and many other forms of entertainment (the era from 1930 to the mid-1950s is commonly called radio's "Golden Age"). Radio was unique among methods of dramatic presentation in that it used only sound.

Audio

A Fisher 500 AM/FM hi-fi receiver from 1959.

AM radio uses amplitude modulation, in which the amplitude of the transmitted signal is made proportional to the sound amplitude captured (transduced) by the microphone, while the transmitted frequency remains unchanged. Transmissions are affected by static and interference because lightning and other sources of radio emissions on the same frequency add their amplitudes to the original transmitted amplitude. In the early part of

the 20th century, American AM radio stations broadcast with powers as high as 500 kW, and some could be heard worldwide; these stations' transmitters were commandeered for military use by the US Government during World War II. Currently, the maximum broadcast power for a civilian AM radio station in the United States and Canada is 50 kW, and the majority of stations that emit signals this powerful were grandfathered in. In 1986 KTNN received the last granted 50,000 watt license. These 50 kW stations are generally called "clear channel" stations (not to be confused with Clear Channel Communications), because within North America each of these stations has exclusive use of its broadcast frequency throughout part or all of the broadcast day.

Bush House, home of the BBC World Service.

FM broadcast radio sends music and voice with higher fidelity than AM radio. In frequency modulation, amplitude variation at the microphone causes the transmitter frequency to fluctuate. Because the audio signal modulates the frequency and not the amplitude, an FM signal is not subject to static and interference in the same way as AM signals. Due to its need for a wider bandwidth, FM is transmitted in the Very High Frequency (VHF, 30 MHz to 300 MHz) radio spectrum. VHF radio waves act more like light, traveling in straight lines; hence the reception range is generally limited to about 50–100 miles. During unusual upper atmospheric conditions, FM signals are occasionally reflected back towards the Earth by the ionosphere, resulting in long distance FM reception. FM receivers are subject to the capture effect, which causes the radio to only receive the strongest signal when multiple signals appear on the same frequency. FM receivers are relatively immune to lightning and spark interference.

High power is useful in penetrating buildings, diffracting around hills, and refracting in the dense atmosphere near the horizon for some distance beyond the horizon. Consequently, 100,000 watt FM stations can regularly be heard up to 100 miles (160 km) away, and farther (e.g., 150 miles, 240 km) if there are no competing signals. A few old,

"grandfathered" stations do not conform to these power rules. WBCT-FM (93.7) in Grand Rapids, Michigan, USA, runs 320,000 watts ERP, and can increase to 500,000 watts ERP by the terms of its original license. Such a huge power level does not usually help to increase range as much as one might expect, because VHF frequencies travel in nearly straight lines over the horizon and off into space. Nevertheless, when there were fewer FM stations competing, this station could be heard near Bloomington, Illinois, USA, almost 300 miles (500 km) away.

FM subcarrier services are secondary signals transmitted in a "piggyback" fashion along with the main program. Special receivers are required to utilize these services. Analog channels may contain alternative programming, such as reading services for the blind, background music or stereo sound signals. In some extremely crowded metropolitan areas, the sub-channel program might be an alternate foreign language radio program for various ethnic groups. Sub-carriers can also transmit digital data, such as station identification, the current song's name, web addresses, or stock quotes. In some countries, FM radios automatically re-tune themselves to the same channel in a different district by using sub-bands.

Aviation voice radios use VHF AM. AM is used so that multiple stations on the same channel can be received. (Use of FM would result in stronger stations blocking out reception of weaker stations due to FM's capture effect). Aircraft fly high enough that their transmitters can be received hundreds of miles (or kilometres) away, even though they are using VHF.

Degen DE1103, an advanced world mini-receiver with single sideband modulation and dual conversion

Marine voice radios can use single sideband voice (SSB) in the shortwave High Frequency (HF—3 MHz to 30 MHz) radio spectrum for very long ranges or narrowband FM in the VHF spectrum for much shorter ranges. Narrowband FM sacrifices fidelity to make more channels available within the radio spectrum, by using a smaller range of radio frequencies, usually with five kHz of deviation, versus the 75 kHz used by commercial FM broadcasts, and 25 kHz used for TV sound.

Government, police, fire and commercial voice services also use narrowband FM on special frequencies. Early police radios used AM receivers to receive one-way dispatches.

Civil and military HF (high frequency) voice services use shortwave radio to contact ships at sea, aircraft and isolated settlements. Most use single sideband voice (SSB), which uses less bandwidth than AM. On an AM radio SSB sounds like ducks quacking, or the adults in a Charlie Brown cartoon. Viewed as a graph of frequency versus power, an AM signal shows power where the frequencies of the voice add and subtract with the main radio frequency. SSB cuts the bandwidth in half by suppressing the carrier and one of the sidebands. This also makes the transmitter about three times more powerful, because it doesn't need to transmit the unused carrier and sideband.

TETRA, Terrestrial Trunked Radio is a digital cell phone system for military, police and ambulances. Commercial services such as XM, WorldSpace and Sirius offer encrypted digital Satellite radio.

Telephony

Mobile phones transmit to a local cell site (transmitter/receiver) that ultimately connects to the public switched telephone network (PSTN) through an optic fiber or microwave radio and other network elements. When the mobile phone nears the edge of the cell site's radio coverage area, the central computer switches the phone to a new cell. Cell phones originally used FM, but now most use various digital modulation schemes. Recent developments in Sweden (such as DROPme) allow for the instant downloading of digital material from a radio broadcast (such as a song) to a mobile phone.

Satellite phones use satellites rather than cell towers to communicate.

Video

Television sends the picture as AM and the sound as AM or FM, with the sound carrier a fixed frequency (4.5 MHz in the NTSC system) away from the video carrier. Analog television also uses a vestigial sideband on the video carrier to reduce the bandwidth required.

Digital television uses 8VSB modulation in North America (under the ATSC digital television standard), and COFDM modulation elsewhere in the world (using the DVB-T standard). A Reed–Solomon error correction code adds redundant correction codes and allows reliable reception during moderate data loss. Although many current and future codecs can be sent in the MPEG transport stream container format, as of 2006 most systems use a standard-definition format almost identical to DVD: MPEG-2 video in Anamorphic widescreen and MPEG layer 2 (*MP2*) audio. High-definition television is possible simply by using a higher-resolution picture, but H.264/AVC is being considered as a replacement video codec in some regions for its improved compression. With the compression and improved modulation involved, a single "channel" can contain a high-definition program and several standard-definition programs.

Navigation

All satellite navigation systems use satellites with precision clocks. The satellite transmits its position, and the time of the transmission. The receiver listens to four satellites, and can figure its position as being on a line that is tangent to a spherical shell around each satellite, determined by the time-of-flight of the radio signals from the satellite. A computer in the receiver does the math.

Radio direction-finding is the oldest form of radio navigation. Before 1960 navigators used movable loop antennas to locate commercial AM stations near cities. In some cases they used marine radiolocation beacons, which share a range of frequencies just above AM radio with amateur radio operators. LORAN systems also used time-of-flight radio signals, but from radio stations on the ground. VOR (Very High Frequency Omnidirectional Range), systems (used by aircraft), have an antenna array that transmits two signals simultaneously. A directional signal rotates like a lighthouse at a fixed rate. When the directional signal is facing north, an omnidirectional signal pulses. By measuring the difference in phase of these two signals, an aircraft can determine its bearing or radial from the station, thus establishing a line of position. An aircraft can get readings from two VORs and locate its position at the intersection of the two radials, known as a "fix." When the VOR station is collocated with DME (Distance Measuring Equipment), the aircraft can determine its bearing and range from the station, thus providing a fix from only one ground station. Such stations are called VOR/DMEs. The military operates a similar system of navaids, called TACANs, which are often built into VOR stations. Such stations are called VORTACs. Because TACANs include distance measuring equipment, VOR/DME and VORTAC stations are identical in navigation potential to civil aircraft.

Radar

Radar (Radio Detection And Ranging) detects objects at a distance by bouncing radio waves off them. The delay caused by the echo measures the distance. The direction of the beam determines the direction of the reflection. The polarization and frequency of the return can sense the type of surface. Navigational radars scan a wide area two to four times per minute. They use very short waves that reflect from earth and stone. They are common on commercial ships and long-distance commercial aircraft.

General purpose radars generally use navigational radar frequencies, but modulate and polarize the pulse so the receiver can determine the type of surface of the reflector. The best general-purpose radars distinguish the rain of heavy storms, as well as land and vehicles. Some can superimpose sonar data and map data from GPS position.

Search radars scan a wide area with pulses of short radio waves. They usually scan the area two to four times a minute. Sometimes search radars use the Doppler effect to separate moving vehicles from clutter. Targeting radars use the same principle as search radar but scan a much smaller area far more often, usually several times a second or more. Weather radars resemble search radars, but use radio waves with circular

polarization and a wavelength to reflect from water droplets. Some weather radar use the Doppler effect to measure wind speeds.

Data (digital radio)

2008 Pure One Classic digital radio

Most new radio systems are digital, The oldest form of digital broadcast was spark gap telegraphy, used by pioneers such as Marconi. By pressing the key, the operator could send messages in Morse code by energizing a rotating commutating spark gap. The rotating commutator produced a tone in the receiver, where a simple spark gap would produce a hiss, indistinguishable from static. Spark-gap transmitters are now illegal, because their transmissions span several hundred megahertz. This is very wasteful of both radio frequencies and power.

The next advance was continuous wave telegraphy, or CW (Continuous Wave), in which a pure radio frequency, produced by a vacuum tube electronic oscillator was switched on and off by a key. A receiver with a local oscillator would "heterodyne" with the pure radio frequency, creating a whistle-like audio tone. CW uses less than 100 Hz of bandwidth. CW is still used, these days primarily by amateur radio operators (hams). Strictly, on-off keying of a carrier should be known as "Interrupted Continuous Wave" or ICW or on-off keying (OOK).

Radio teletypes usually operate on short-wave (HF) and are much loved by the military because they create written information without a skilled operator. They send a bit as one of two tones. Groups of five or seven bits become a character printed by a teletype. From about 1925 to 1975, radio teletype was how most commercial messages were sent to less developed countries. These are still used by the military and weather services.

Aircraft use a 1200 Baud radioteletype service over VHF to send their ID, altitude and position, and get gate and connecting-flight data. Microwave dishes on satellites, telephone exchanges and TV stations usually use quadrature amplitude modulation (QAM). QAM sends data by changing both the phase and the amplitude of the radio signal. Engineers like QAM because it packs the most bits into a radio signal when given an exclusive (non-shared) fixed narrowband frequency range. Usually the bits are sent in "frames" that repeat. A special bit pattern is used to locate the beginning of a frame.

Modern GPS receivers.

Communication systems that limit themselves to a fixed narrowband frequency range are vulnerable to jamming. A variety of jamming-resistant spread spectrum techniques were initially developed for military use, most famously for Global Positioning System satellite transmissions. Commercial use of spread spectrum began in the 1980s. Bluetooth, most cell phones, and the 802.11b version of Wi-Fi each use various forms of spread spectrum.

Systems that need reliability, or that share their frequency with other services, may use "coded orthogonal frequency-division multiplexing" or COFDM. COFDM breaks a digital signal into as many as several hundred slower subchannels. The digital signal is often sent as QAM on the subchannels. Modern COFDM systems use a small computer to make and decode the signal with digital signal processing, which is more flexible and far less expensive than older systems that implemented separate electronic channels. COFDM resists fading and ghosting because the narrow-channel QAM signals can be sent slowly. An adaptive system, or one that sends error-correction codes can also resist interference, because most interference can affect only a few of the QAM channels. COFDM is used for Wi-Fi, some cell phones, Digital Radio Mondiale, Eureka 147, and many other local area network, digital TV and radio standards.

Heating

Radio-frequency energy generated for heating of objects is generally not intended to radiate outside of the generating equipment, to prevent interference with other radio signals. Microwave ovens use intense radio waves to heat food. Diathermy equipment is used in surgery for sealing of blood vessels. Induction furnaces are used for melting metal for casting, and induction hobs for cooking.

Amateur radio service

Amateur radio station with multiple receivers and transceivers

Amateur radio, also known as "ham radio", is a hobby in which enthusiasts are licensed to communicate on a number of bands in the radio frequency spectrum non-commercially and for their own enjoyment. They may also provide emergency and public service assistance. This has been very beneficial in emergencies, saving lives in many instances. Radio amateurs use a variety of modes, including nostalgic ones like Morse code and experimental ones like Low-Frequency Experimental Radio. Several forms of radio were pioneered by radio amateurs and later became commercially important, including FM, single-sideband (SSB), AM, digital packet radio and satellite repeaters. Some amateur frequencies may be disrupted by power-line internet service.

Unlicensed radio services

Unlicensed, government-authorized personal radio services such as Citizens' band radio in Australia, the USA, and Europe, and Family Radio Service and Multi-Use Radio Service in North America exist to provide simple, (usually) short range communication for individuals and small groups, without the overhead of licensing. Similar services exist in other parts of the world. These radio services involve the use of handheld units.

Free radio stations, sometimes called pirate radio or "clandestine" stations, are unauthorized, unlicensed, illegal broadcasting stations. These are often low power transmitters operated on sporadic schedules by hobbyists, community activists, or political and cultural dissidents. Some pirate stations operating offshore in parts of Europe and the United Kingdom more closely resembled legal stations, maintaining regular schedules, using high power, and selling commercial advertising time.

Radio control (R C)

Radio remote controls use radio waves to transmit control data to a remote object as in some early forms of guided missile, some early TV remotes and a range of model boats, cars and airplanes. Large industrial remote-controlled equipment such as cranes and switching locomotives now usually use digital radio techniques to ensure safety and reliability.

In Madison Square Garden, at the Electrical Exhibition of 1898, Nikola Tesla successfully demonstrated a radio-controlled boat. He was awarded U.S. patent No. 613,809 for a "Method of and Apparatus for Controlling Mechanism of Moving Vessels or Vehicles."

Chapter 5

Wi-Fi Technologies

Wi-Fi refers to a range of connectivity technologies including wireless local area network (WLAN) based on the IEEE 802.11 standards, device to device connectivity [such as Wi-Fi Peer to Peer AKA Wi-Fi Direct], and a range of technologies that support PAN, LAN and even Wide Area Network (WAN) connections. IEEE 802.11 has been used interchangeably with Wi-Fi, however Wi-Fi has become a superset of IEEE 802.11 over the past few years. Wi-Fi is used by over 700 million people, there are over 750,000 hotspots (places with Wi-Fi internet connectivity) around the world, and about 800 million new Wi-Fi devices every year. Wi-Fi products that complete the Wi-Fi Alliance interoperability certification testing successfully can use the Wi-Fi CERTIFIED designation and trademark.

Not every Wi-Fi device is submitted for certification to the Wi-Fi Alliance. The lack of Wi-Fi certification does not necessarily imply a device is incompatible with Wi-Fi devices.

Wi-Fi devices are installed in many personal computers, video game consoles, MP3 players, smartphones, printers, and other peripherals, and newer laptop computers.

Wi-Fi certification

Wi-Fi technology builds on IEEE 802.11 standards. The IEEE develops and publishes some these standards, but does not test equipment for compliance with them. The non-profit Wi-Fi Alliance formed in 1999 to fill this void — to establish and enforce standards for interoperability and backward compatibility, and to promote wireless local-area-network technology. As of 2010 the Wi-Fi Alliance consisted of more than 375 companies from around the world. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo.

Specifically, the certification process requires conformance to the IEEE 802.11 radio standards, the WPA and WPA2 security standards, and the EAP authentication standard. Certification may optionally include tests of IEEE 802.11 draft standards, interaction with cellular-phone technology in converged devices, and features relating to security set-up, multimedia, and power-saving.

Most recently, a new security standard, Wi-Fi Protected Setup, allows embedded devices with limited graphical user interface to connect to the Internet with ease. Wi-Fi Protected Setup has 2 configurations: The Push Button configuration and the PIN configuration. These embedded devices are also called The Internet of Things and are low-power, battery-operated embedded systems. A number of WiFi manufacturers design chips and modules for embedded Wi-Fi, such as GainSpan.

The name *Wi-Fi*

The term *Wi-Fi* suggests *Wireless Fidelity*, resembling the long-established audio-equipment classification term *high fidelity* (in use since the 1930s) or *Hi-Fi* (used since 1950). Even the Wi-Fi Alliance itself has often used the phrase *Wireless Fidelity* in its press releases and documents; the term also appears in a white paper on Wi-Fi from ITAA. However, based on Phil Belanger's statement, the term Wi-Fi was never supposed to mean anything at all.

The term *Wi-Fi*, first used commercially in August 1999, was coined by a brand-consulting firm called Interbrand Corporation that the Alliance had hired to determine a name that was "a little catchier than 'IEEE 802.11b Direct Sequence'". Belanger also stated that Interbrand invented *Wi-Fi* as a play on words with *Hi-Fi*, and also created the yin-yang-style Wi-Fi logo.

The Wi-Fi Alliance initially used an advertising slogan for Wi-Fi, "The Standard for Wireless Fidelity", but later removed the phrase from their marketing. Despite this, some documents from the Alliance dated 2003 and 2004 still contain the term *Wireless Fidelity*. There was no official statement related to the dropping of the term.

The yin-yang logo indicates the certification of a product for interoperability.

Uses

Internet access

A roof-mounted Wi-Fi antenna

A Wi-Fi enabled device such as a personal computer, video game console, smartphone or digital audio player can connect to the Internet when within range of a wireless network connected to the Internet. The coverage of one or more (interconnected) access points — called hotspots — can comprise an area as small as a few rooms or as large as many square miles. Coverage in the larger area may depend on a group of access points with

overlapping coverage. Wi-Fi technology has been used in wireless mesh networks, for example, in London, UK.

In addition to private use in homes and offices, Wi-Fi can provide public access at Wi-Fi hotspots provided either free-of-charge or to subscribers to various commercial services. Organizations and businesses - such as those running airports, hotels and restaurants - often provide free-use hotspots to attract or assist clients. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. As of 2008 more than 300 metropolitan-wide Wi-Fi (Muni-Fi) projects had started. As of 2010 the Czech Republic had 1150 Wi-Fi based wireless Internet service providers.

Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other premises, can provide Internet access and internetworking to all devices connected (wirelessly or by cable) to them. With the emergence of MiFi and WiBro (a portable Wi-Fi router) people can easily create their own Wi-Fi hotspots that connect to Internet via cellular networks. Now many mobile phones can also create wireless connections via tethering on iPhone, Android, Symbian, and WinMo.

One can also connect Wi-Fi devices in ad-hoc mode for client-to-client connections without a router. Wi-Fi also connects places that would traditionally not have network access, for example bathrooms, kitchens and garden sheds.

Municipal wireless network

Municipal wireless network (**Municipal Wi-Fi**, **Muni Wi-Fi** or **Muni-Fi**) is the concept of turning an entire city into a Wireless Access Zone (WAZ), with the ultimate goal of making wireless access to the Internet a universal service. This is usually done by providing municipal broadband via Wi-Fi to large parts or all of a municipal area by deploying a wireless mesh network. The typical deployment design uses hundreds of routers deployed outdoors, often on utility poles. The operator of the network acts as a wireless internet service provider.

Overview

A municipal Wi-Fi antenna in Minneapolis, MN.

Such networks go far beyond the existing piggybacking opportunities available near public libraries and some coffee shops. The basic premise of carpeting an area with wireless service in urban centers is that it is more economical to the community to provide the service as a utility rather than to have individual households and businesses pay private firms for such a service. Such networks are viewed as capable of enhancing city management and public safety, especially when used directly by city employees out in the field. They can also be viewed as a social service to those who cannot afford private high-speed services such as DSL. When the network service is free and a small number of clients consume a majority of the available capacity, operating and regulating the network might prove difficult.

The US Federal Trade Commission has expressed some concerns about such private/public partnerships as trending towards a franchise monopoly.

Technology continues to advance. In 2007, companies with existing cell sites offered competing paid high-speed wireless services where the laptop owner purchased a PC card or adapter which uses communications based on EV-DO cellular data receivers or

WiMAX rather than 802.11b/g. High-end laptops in 2007 feature built-in support for these newer protocols. The next generation of Intel Centrino will support dual Wi-Fi and WiMAX. WiMAX is designed to implement a metropolitan area network (MAN) while 802.11 is designed to implement a wireless local area network (LAN).

2010 ushers in the potential for what is being called “super WiFi” or "white spots.” In September 2010, the FCC announced that radio spectrum formerly only available to television stations would be opened for public use, carrying with it the potential for increased WiFi range and decreases in cost, and potentially making it easier to offer rural areas broadband Internet access.

Within the United States, providing a municipal wireless network is not officially recognized as a priority. Some have argued that the benefits of public approach may exceed the costs, similar to cable television.

Finance

The construction of such networks is a significant part of their lifetime costs. Usually, a private firm works closely with local government to construct such a network and operate it. Financing is usually shared by both the private firm and the municipal government. Once operational, the service may be free, supported by advertising, provided for a monthly charge per user or some combination. Among deployed networks, usage as measured by number of distinct users has been shown to be moderate to light. Private firms serving multiple cities sometimes maintain a single account for each user thus allowing the user a limited amount of portable service as they travel among the cities covered by the firm. As of 2007, some Muni WiFi deployments are delayed as the private and public partners involved in planned networks continue to negotiate the business model and financing.

In the build-out of such networks, radio communication is used both for the Wi-Fi service and for the "backhaul" or pathway to the Internet. This means that the nodes only need a wire for power (hence the habit of installing them on power and light utility poles). This "all radio" approach means that nodes must be within range of each other and form a contiguous pathway back to special aggregation nodes that have more traditional access to the Internet. Nodes then relay traffic, somewhat like a fire-bucket brigade, from the laptop to the aggregation node. This limits the way in which the network can be grown incrementally: coverage starts near the aggregation point and, as the mesh grows, new coverage can only grow out from the edge of the mesh. If a new, isolated area is to be covered, then a new aggregation point must be constructed. Private firms often take a phased approach, starting with one or a few sectors of a city to demonstrate competence before making the larger investment of attempting full coverage of a city.

Google WiFi is entirely funded by Google. Despite a failed attempt to provide citywide WiFi through a partnership with internet service provider Earthlink in 2007, the company claims that they are currently working to provide a wireless network for the city of San Francisco, California, although there is no specified completion date. Some other projects

that are still in the planning stages have pared back their planned coverage from 100% of a municipal area to only densely commercially zoned areas. One of the most ambitious planned projects is to provide wireless service throughout Silicon Valley, but the winner of the bid seems ready to request that the 40 cities involved help cover more of the cost which has raised concerns that the project will ultimately be too slow-to-market to be deemed a success. Advances in technology in 2005-2007 may allow wireless community network projects to offer a viable alternative. Such projects have an advantage that as they do not have to negotiate with government entities they have no contractual obligations for coverage. A promising example is Meraki's demonstration in San Francisco, which already claims 20,000 distinct users as of October 2007.

In 2009, Microsoft and Yahoo also provided free wireless to select regions in the United States. Yahoo's free WiFi was made available for one full year to the Times Square area in New York City beginning November 10, 2009. Microsoft made free WiFi available to select airports and hotels across the United States, in exchange for one search on the Bing search engine by the user.

Campus-wide Wi-Fi

Carnegie Mellon University built the first wireless Internet network in the world at their Pittsburgh campus in 1994, long before Wi-Fi branding originated in 1999. Most campuses now have wireless Internet.

Drexel University in Philadelphia made history by becoming the United State's first major university to offer completely wireless Internet access across the entire campus in 2000.

Direct computer-to-computer communications

Wi-Fi also allows communications directly from one computer to another without the involvement of an access point. This is called the *ad-hoc* mode of Wi-Fi transmission. This wireless ad-hoc network mode has proven popular with multiplayer handheld game consoles, such as the Nintendo DS, digital cameras, and other consumer electronics devices.

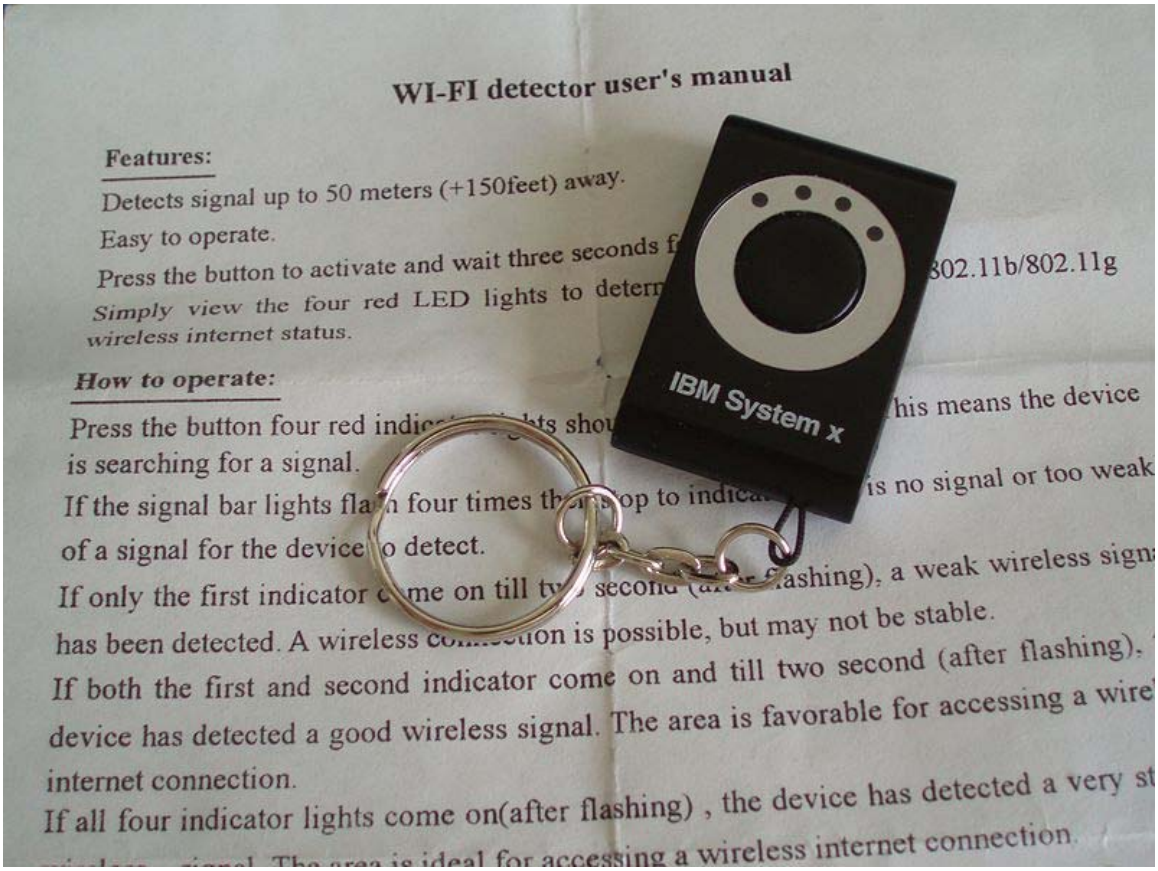
Similarly, the Wi-Fi Alliance promotes a pending specification called *Wi-Fi Direct* for file transfers and media sharing through a new discovery- and security-methodology.

Future directions

As of 2010 Wi-Fi technology has spread widely within business and industrial sites. In business environments, just like other environments, increasing the number of Wi-Fi access points provides network redundancy, support for fast roaming and increased overall network-capacity by using more channels or by defining smaller cells. Wi-Fi enables wireless voice-applications (VoWLAN or WVOIP). Over the years, Wi-Fi implementations have moved toward "thin" access points, with more of the network

intelligence housed in a centralized network appliance, relegating individual access points to the role of "dumb" transceivers. Outdoor applications may utilize mesh topologies.

Advantages and challenges



A keychain-size Wi-Fi detector

Operational advantages

Wi-Fi allows the deployment of local area networks (LANs) without wires for client devices, 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.

As of 2010 manufacturers are building wireless network adapters into most laptops. The price of chipsets for Wi-Fi continues to drop, making it an economical networking option included in even more devices. Wi-Fi has become widespread in corporate infrastructures.

Different competitive brands of access points and client network-interfaces can inter-operate at a basic level of service. Products designated as "Wi-Fi Certified" by the Wi-Fi Alliance are backwards compatible. "Wi-Fi" designates a globally operative set of standards: unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.

Wi-Fi operates in more than 220,000 public hotspots and in tens of millions of homes and corporate and university campuses worldwide. The current version of Wi-Fi Protected Access encryption (WPA2) as of 2010 is considered secure, provided users employ a strong passphrase. New protocols for quality-of-service (WMM) make Wi-Fi more suitable for latency-sensitive applications (such as voice and video); and power saving mechanisms (WMM Power Save) improve battery operation.

Limitations

Spectrum assignments and operational limitations do not operate consistently worldwide. Most of Europe allows for an additional 2 channels beyond those permitted in the U.S. for the 2.4 GHz band. (1–13 vs. 1–11); Japan has one more on top of that (1–14). Europe, as of 2007, was essentially homogeneous in this respect. A very confusing aspect is the fact that a Wi-Fi signal actually occupies five channels in the 2.4 GHz band resulting in only three non-overlapped channels in the U.S.: 1, 6, 11, and three or four in Europe: 1, 5, 9, 13. Equivalent isotropically radiated power (EIRP) in the EU is limited to 20 dBm (100 mW).

Reach

Long-range Wi-Fi

Large satellite dish used for long-range Wi-Fi connection in Venezuela

Long-range Wi-Fi is used for low-cost, unregulated point-to-point connections, as an alternative to cellular networks or satellite links.

Introduction

Since the development of the Wi-Fi radio standard, great leaps in the technology have been made. In the area of range Wi-Fi has been pushed to an extreme, and both commercial and residential applications of this Long Range Wi-Fi have cropped up around the world. It has also been used in experimental trials in the developing world to link communities separated by difficult geography with few or no other connectivity options.

Applications

Business

- Provide coverage to a large office or business complex or campus.
- Establish point-to-point link between large skyscrapers or other office buildings.
- Bring Internet to remote construction sites or research labs.

Residential

- Bring Internet to a home if regular cable/DSL cannot be hooked up at the location.
- Bring Internet to a vacation home or cottage on a remote mountain or on a lake.
- Bring Internet to a yacht or large seafaring vessel.
- Share a neighborhood Wi-Fi network.

Large-scale deployments

The (TIER) project at University of California at Berkeley, in collaboration with Intel, utilizes a modified Wi-Fi setup to create long-distance point-to-point links for several of its projects in the developing world. This technique, dubbed Wi-Fi over Long Distance (WiLD), is used to connect the Aravind Eye Hospital with several outlying clinics in Tamil Nadu state, India. Distances range from five (5) to over fifteen (15) kilometers (3–10 miles) with stations placed in line of sight of each other. These links allow specialists at the hospital to communicate with nurses and patients at the clinics through video conferencing. If the patient needs further examination or care, a hospital appointment can then be scheduled. Another network in Ghana links the University of Ghana, Legon campus to its remote campuses at the Korle bu Medical School and the City campus; a further extension will feature links up to 80 km (50 mi) apart.

The Tegola project of the University of Edinburgh, is developing new technologies to bring high-speed, affordable broadband to rural areas beyond the reach of fibre. A 5-link ring connects Knoydart, the N. shore of Loch Hourne, and a remote community at Kilbeg to backhaul from the Gaelic College on Skye. All links pass over tidal waters; they range in length from 2.5 km to 19 km.

Increasing range in other ways

Specialized Wi-Fi channels

In most standard Wi-Fi routers, the three standards, a, b and g, are enough. But in long-range Wi-Fi, special technologies are used to get the most out of a Wi-Fi connection. The 802.11-2007 standard adds 10 MHz and 5 MHz OFDM modes to the 802.11a standard, and extend the time of cyclic prefix protection from 0.8 μs to 3.2 μs, quadrupling the

multipath distortion protection. Some commonly available 802.11a/g chipsets support the OFDM 'half-clocking' and 'quarter-clocking' that is in the 2007 standard, and 4.9 GHz and 5.0 GHz products are available with 10 MHz and 5 MHz channel bandwidths. It is likely that some 802.11n D.20 chipsets will also support 'half-clocking' for use in 10 MHz channel bandwidths, and at double the range of the 802.11n standard.

802.11n and MIMO

Preliminary 802.11n working became available in many routers in 2008. This technology can use multiple antennas to target one or more sources to increase speed. This is known as MIMO, Multiple Input Multiple Output. In tests, the speed increase was said to only occur over short distances rather than the long range needed for most point to point setups. On the other hand, using dual antennas with orthogonal polarities along with a 2x2 MIMO chipset effectively enable two independent carrier signals to be sent and received along the same long distance path.

Power increase or receiver sensitivity boosting

A rooftop 1 watt WiFi amp, feeding a simple antenna

Another way of adding range uses a power amplifier. Commonly known as "range extender amplifiers" these small devices supply usually around ½ watt of power to the antenna. Such amplifiers may give more than five times the range to an existing network. Every 6 dB gain doubles range. The alternative techniques of selecting a more sensitive WLAN adapter (some are quite "deaf") and more directive antenna should also be considered.

Higher gain antennas and adapter placement

Specially shaped directional antennas can be used to increase the range of a Wi-Fi transmission without a drastic increase in transmission power. High gain antenna may be of many designs, but all allow transmitting a narrow signal beam over distances of several kilometers, often nulling out nearby interference sources. A popular low-cost home made approach increases WiFi ranges by just placing standard USB WLAN hardware at the focal point of modified parabolic cookware. Such "WokFi" techniques typically yield gains of 12–15 dB over the bare system—enough for line of sight (LOS) ranges of several kilometers and improvements in marginal locations. N.B. Although often low power, cheap USB WLAN adapters suit site auditing and location of local signal "sweet spots". As USB leads incur none of the losses normally associated with costly microwave coax and SMA fittings, just extending a USB adapter (or AP, etc.) up to a window, or away from shielding metal work and vegetation, may dramatically improve the link.

Protocol hacking

The standard IEEE 802.11 protocol stacks can also be modified to make them more suitable for long distance, point-to-point usage, at the risk of breaking interoperability with other Wi-Fi devices and suffering interference from transmitters located near the antenna. These approaches are used by the TIER project.

In addition to power levels it is also important to know how the 802.11 protocol uses acknowledge for each received frame. If acknowledge is not received the frame is re-transmitted. By default the maximum distance between transmitter and receiver is 1 mile (1.6 km). On longer distances the delay will force retransmissions. On some professional equipment such as Cisco Aironet 1200 this parameter can be tuned for optimal throughput.

Packet Fragmentation can also be used to improve throughput in noisy/congested situations. Although packet fragmentation is often thought of as something bad, and does indeed add a large overhead, reducing throughput, sometimes it is necessary. For example, in a congested situation, ping times of 30 byte packets can be excellent, whilst ping times of 1450 byte packets can be very poor with high packet loss. Dividing the packet into two, by setting a fragmentation threshold to 750, can vastly improve the throughput. The fragmentation threshold should be a division of the MTU, typically 1500, so should be 750, 500, 375, etc. However, excessive fragmentation can make the problem worse, since the increased overhead will increase congestion.

Obstacles to long-range Wi-Fi

Methods that stretch the range of a Wi-Fi connection may also make it fragile and volatile, due to mundane problems including:

Landscape interference

Obstacles are among the biggest problems when setting up a long-range Wi-Fi. Trees and forests degrade the microwave signal, and rolling hills make it difficult to establish line-of-sight propagation.

In a city, buildings will impact integrity, speed and connectivity. Steel frames partly reflect radio signals, and concrete or plaster walls absorb microwave signals significantly, but sheet metal in walls or roofs may efficiently *reflect* Wi-Fi signals, causing an almost total loss of signal.

Tidal fading

Where point-to-point wire- less links are deployed at low altitudes over tidal estuaries, multipath interference from reflections over tidal water can be constructive at some states of tide and destructive at others. The Tegola project uses a slow frequency-hopping technique to mitigate tidal fading.

2.4 GHz interference

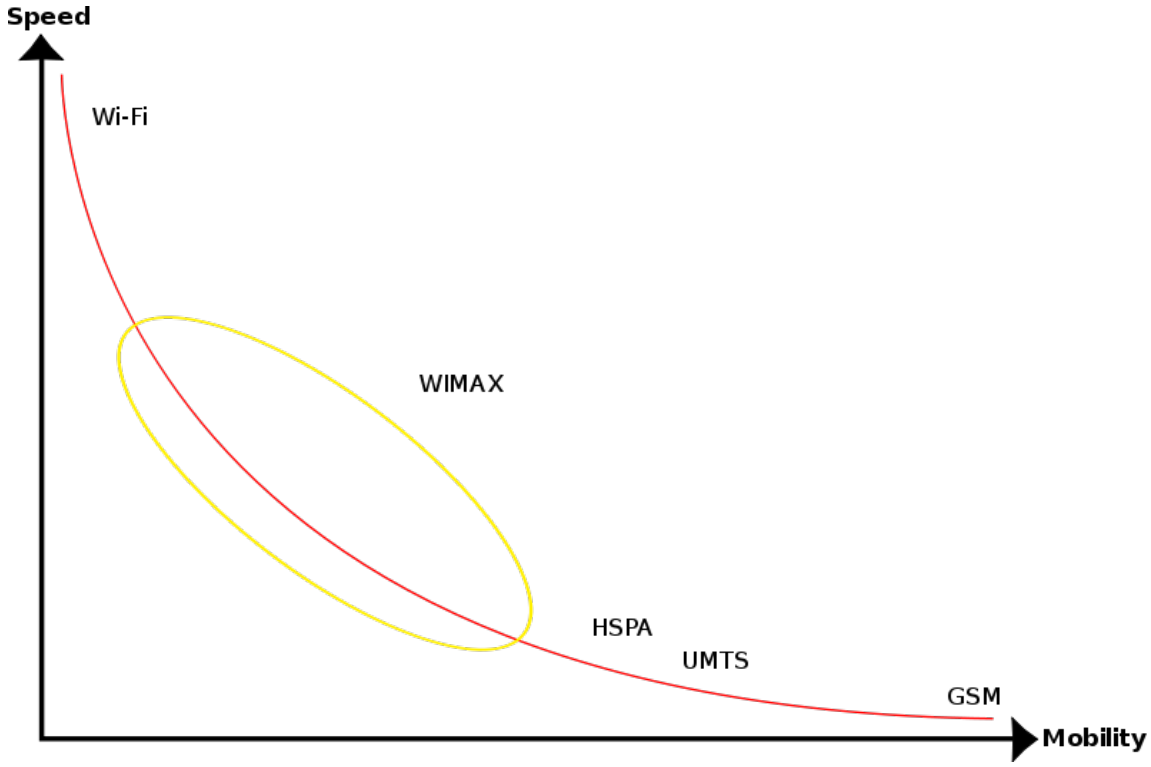
Microwave ovens in residences dominate the 2.4 GHz band and will cause "meal time perturbations" of the noise floor. There are literally hundreds of other sources of interference that aggregate into a formidable obstacle to enabling long range use in occupied areas: baby monitors, wireless cameras, remote car starters, DECT and residential wireless phones, Bluetooth products to name just a few.

Due to the intended nature of the 2.4 GHz band, there are many users of this band, with as many as 2 or 3 devices per household. By its very nature, "Long Range Wifi" connotes an antenna system which can see many of these devices, which when added together produce a very high noise floor, whereby no single signal is usable, but nonetheless are still received. The aim of a long range system is to produce a system which over-powers these signals and/or uses directional antennas to prevent the receiver "seeing" these devices, thereby reducing the noise floor.

Several of the devices on the market are not legal in the UK. The UK appears to have particularly specific and strict regulations regarding the 2.4 GHz band. In many other countries, anything with 100 mW EIRP is considered "fair game". However, in the UK, there are extremely strict and specific regulations as to what can and cannot be used and sold on 2.4 GHz. The most notable difference in the UK is that video senders can only have a 10 mW EIRP, and must dissipate the transmitted signal across 20 MHz.

More information about 2.4 GHz interference can be found on the article Electromagnetic interference at 2.4 GHz, which lists the different types of appliances on 2.4 GHz, and how they interfere with each other.

Mobility



Speed vs. Mobility of wireless systems: Wi-Fi, HSPA, UMTS, GSM

The very limited practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces, barcode-reading devices at check-out stands, or receiving/shipping stations. Mobile use of Wi-Fi over wider ranges is limited, for instance, to uses such as in an automobile moving from one hotspot to another (known as Wardriving). Other wireless technologies are more suitable as illustrated in the graphic.

Data security risks

The most common wireless encryption-standard, Wired Equivalent Privacy (WEP), has been shown to be easily breakable even when correctly configured. Wi-Fi Protected Access (WPA and WPA2) encryption, which became available in devices in 2003, aimed to solve this problem. Wi-Fi access points typically default to an encryption-free (*open*) mode. Novice users benefit from a zero-configuration device that works out-of-the-box, but this default does not enable any wireless security, providing open wireless access to a LAN. To turn security on requires the user to configure the device, usually via a software graphical user interface (GUI). On unencrypted Wi-Fi networks connecting devices can monitor and record data (including personal information), but such networks may use other means of protection, such as a virtual private network or secure Hypertext Transfer Protocol (HTTPS) and Transport Layer Security.

Population

Many 2.4 GHz 802.11b and 802.11g access-points default to the same channel on initial startup, contributing to congestion on certain channels. To change the channel of operation for an access point requires the user to configure the device.

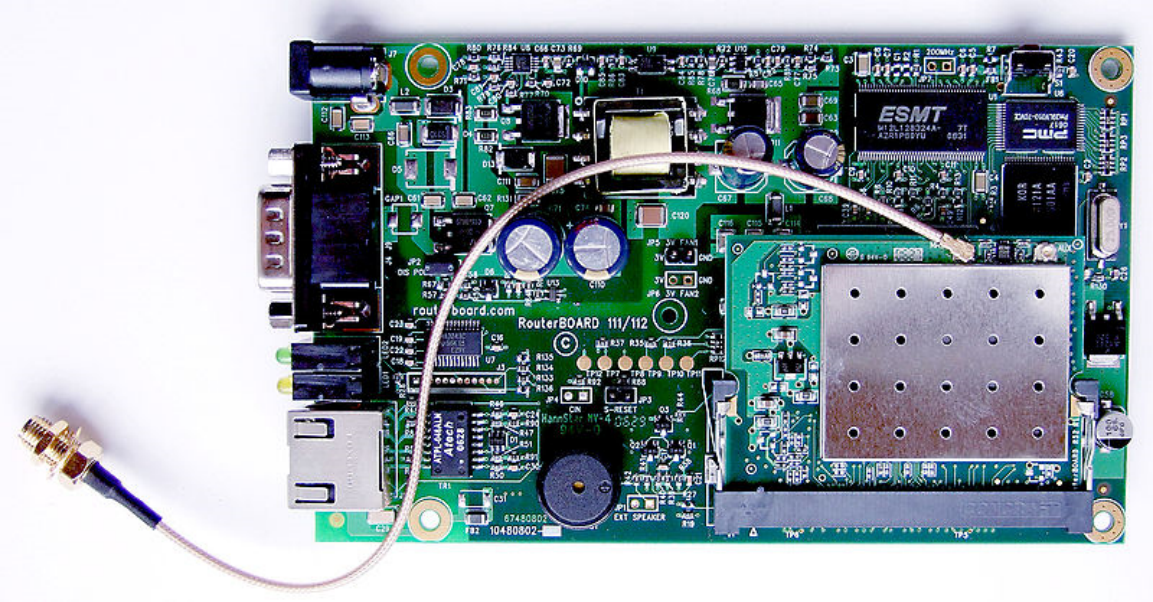
Channel pollution

Market forces may drive a process of standardization. Interoperability issues between non-Wi-Fi brands or proprietary deviations from the standard can still disrupt connections or lower throughput speeds on all devices within range, including any non-Wi-Fi or proprietary product. Moreover, the usage of the ISM band in the 2.45 GHz range is also common to Bluetooth, WPAN-CSS, ZigBee, and any new system will take its share.

Wi-Fi pollution, or an excessive number of access points in the area, especially on the same or neighboring channel, can prevent access and interfere with other devices' use of other access points, caused by overlapping channels in the 802.11g/b spectrum, as well as with decreased signal-to-noise ratio (SNR) between access points. This can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Additionally, other devices use the 2.4 GHz band: microwave ovens, security cameras, ZigBee devices, Bluetooth devices and (in some countries) Amateur radio, video senders, cordless phones and baby monitors, all of which can cause significant additional interference. It is also an issue when municipalities or other large entities (such as universities) seek to provide large area coverage. This the wifi is also called wireless net

Hardware

Standard devices



An embedded RouterBoard 112 with U.FL-RSMA pigtail and R52 mini PCI Wi-Fi card widely used by wireless Internet service providers (WISPs) in the Czech Republic

OSBRiDGE 3GN - 802.11n Access Point and UMTS/GSM Gateway in one device

USB wireless adapter

A wireless access point (WAP) connects a group of wireless devices to an adjacent wired LAN. An access point resembles a network hub, relaying data between connected wireless devices in addition to a (usually) single connected wired device, most often an ethernet hub or switch, allowing wireless devices to communicate with other wired devices.

Wireless adapters allow devices to connect to a wireless network. These adapters connect to devices using various external or internal interconnects such as PCI, miniPCI, USB, ExpressCard, Cardbus and PC Card. As of 2010, most newer laptop computers come equipped with internal adapters. Internal cards are generally more difficult to install.

Wireless routers integrate a Wireless Access Point, ethernet switch, and internal router firmware application that provides IP routing, NAT, and DNS forwarding through an integrated WAN-interface. A wireless router allows wired and wireless ethernet LAN devices to connect to a (usually) single WAN device such as a cable modem or a DSL modem. A wireless router allows all three devices, mainly the access point and router, to be configured through one central utility. This utility is usually an integrated web server that is accessible to wired and wireless LAN clients and often optionally to WAN clients. This utility may also be an application that is run on a desktop computer such as Apple's AirPort.

Wireless network bridges connect a wired network to a wireless network. A bridge differs from an access point: 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.

Wireless range-extenders or wireless repeaters can extend the range of an existing wireless network. Strategically placed range-extenders can elongate a signal area or allow for the signal area to reach around barriers such as those pertaining in L-shaped corridors. Wireless devices connected through repeaters will suffer from an increased latency for each hop. Additionally, a wireless device connected to any of the repeaters in the chain will have a throughput limited by the "weakest link" between the two nodes in the chain from which the connection originates to where the connection ends.

Distance records

Distance records (using non-standard devices) include 382 km (237 mi) in June 2007, held by Ermanno Pietrosemoli and EsLaRed of Venezuela, transferring about 3 MB of data between the mountain-tops of El Águila and Platillon. The Swedish Space Agency transferred data 420 km (260 mi), using 6 watt amplifiers to reach an overhead stratospheric balloon.

Embedded systems

Embedded serial-to-Wi-Fi module

Increasingly in the last few years (particularly as of 2007), embedded Wi-Fi modules have become available that incorporate a real-time operating system and provide a simple means of wirelessly enabling any device which has and communicates via a serial port. This allows the design of simple monitoring devices. An example is a portable ECG device monitoring a patient at home. This Wi-Fi-enabled device can communicate via the Internet.

These Wi-Fi modules are designed so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

Network security

The main issue with wireless network security is its simplified access to the network compared to traditional wired networks such as ethernet. With wired networking one must either gain access to a building (physically connecting into the internal network) or

break through an external firewall. Most business networks protect sensitive data and systems by attempting to disallow external access. Enabling wireless connectivity provides an attack vector, particularly if the network uses inadequate or no encryption.

An attacker who has gained access to a Wi-Fi network router can initiate a DNS spoofing attack against any other user of the network by forging a response before the queried DNS server has a chance to reply.

Securing methods

A common but unproductive measure to deter unauthorized users involves suppressing the access point's SSID broadcast. This is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another unproductive method is to only allow computers with known MAC addresses to join the network. But intruders can defeat this method because they can often (though not always) set MAC addresses with minimal effort (MAC spoofing). If eavesdroppers have the ability to change their MAC address, then they may join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping, but is now deprecated. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys. Once it has seen 5-10 million encrypted packets, AirSnort can determine the encryption password in under a second; newer tools such as aircrack-ptw can use Klein's attack to crack a WEP key with a 50% success rate using only 40,000 packets.

To counteract this in 2002, the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses TKIP as a stopgap solution for legacy equipment. Though more secure than WEP, it has outlived its designed lifetime and has known attack vectors.

In 2004, the IEEE ratified the full IEEE 802.11i (WPA2) encryption standards. If used with a 802.1X server or in pre-shared key mode with a strong and uncommon passphrase WPA2 is still considered[] secure, as of 2009.

Piggybacking

Piggybacking refers to access to a wireless Internet connection by bringing one's own computer within the range of another's wireless connection, and using that service without the subscriber's explicit permission or knowledge.

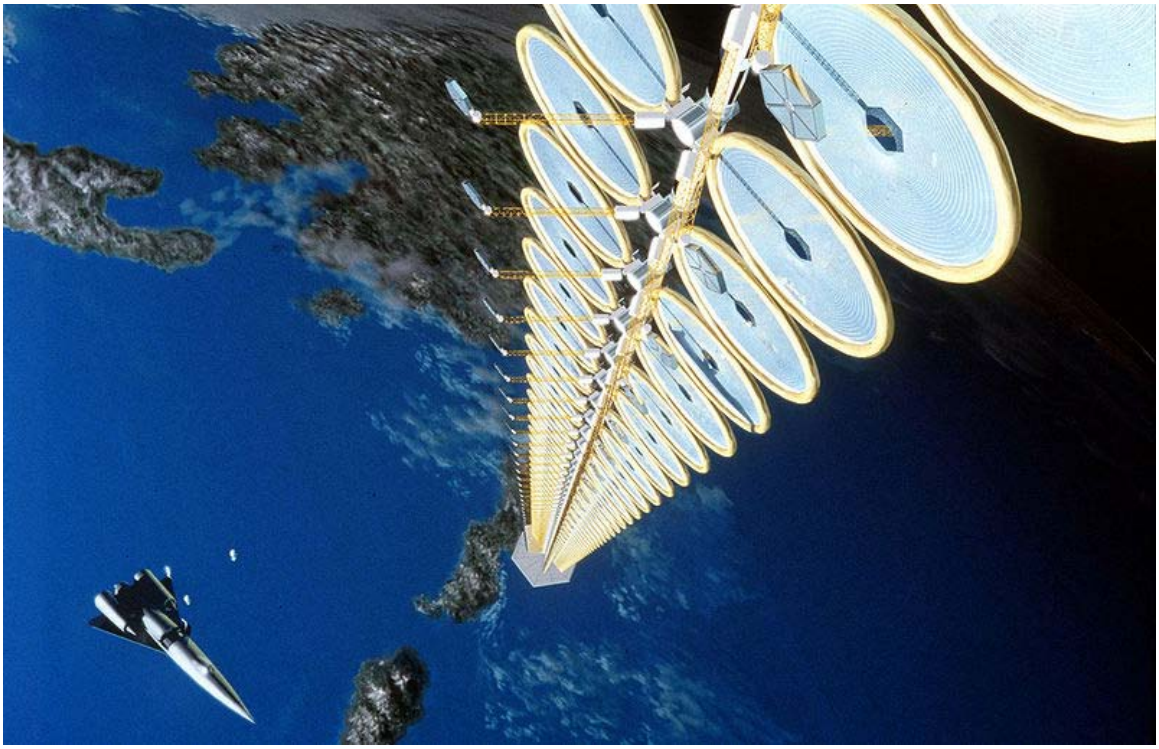
During the early popular adoption of 802.11, providing open access points for anyone within range to use was encouraged to cultivate wireless community networks, particularly since people on average use only a fraction of their downstream bandwidth at any given time.

Recreational logging and mapping of other people's access points has become known as wardriving. Indeed, many access points are intentionally installed without security turned on so that they can be used as a free service. Providing access to one's Internet connection in this fashion may breach the Terms of Service or contract with the ISP. These activities do not result in sanctions in most jurisdictions; however, legislation and case law differ considerably across the world. A proposal to leave graffiti describing available services was called warchalking. A Florida court case determined that owner laziness was not to be a valid excuse.

Piggybacking often occurs unintentionally, most access points are configured without encryption by default, and operating systems can be configured to connect automatically to any available wireless network. A user who happens to start up a laptop in the vicinity of an access point may find the computer has joined the network without any visible indication. Moreover, a user intending to join one network may instead end up on another one if the latter has a stronger signal. In combination with automatic discovery of other network resources this could possibly lead wireless users to send sensitive data to the wrong middle-man when seeking a destination. For example, a user could inadvertently use an insecure network to log in to a website, thereby making the login credentials available to anyone listening, if the website uses an insecure protocol such as HTTP.

Chapter 6

Wireless Energy Transfer



An artist's depiction of a solar satellite, which could send energy wirelessly to a space vessel or planetary surface.

Wireless energy transfer or *Wireless Power* is the process that takes place in any system where electrical energy is transmitted from a power source to an electrical load without interconnecting wires. Wireless transmission is useful in cases where instantaneous or continuous energy transfer is needed but interconnecting wires are inconvenient, hazardous, or impossible.

Wireless energy transfer is different from wireless transmission of information, such as radio, where the signal-to-noise ratio (SNR) or the percentage of power received becomes

critical only if it is too low to adequately recover the signal. With wireless power transmission, efficiency is the more important parameter.

The most common form of wireless power transmission is carried out using induction, followed by electrodynamic induction. Other present-day technologies for wireless power include those based upon microwaves and lasers.

History of wireless energy transfer

- **1820**: André-Marie Ampère develops Ampere's law showing that electric current produces a magnetic field.
- **1831**: Michael Faraday develops Faraday's law of induction describing the electromagnetic force induced in a conductor by a time-varying magnetic flux.
- **1864**: James Clerk Maxwell synthesizes the previous observations, experiments and equations of electricity, magnetism and optics into a consistent theory and mathematically models the behavior of electromagnetic radiation.
- **1888**: Heinrich Rudolf Hertz confirms the existence of electromagnetic radiation. Hertz's "*apparatus for generating electromagnetic waves*" was a VHF or UHF "radio wave" spark gap transmitter.
- **1891**: Nikola Tesla improves Hertz-wave wireless transmitter RF power supply or exciter in his patent No. 454,622, "System of Electric Lighting."
- **1893**: Tesla demonstrates the wireless illumination of phosphorescent lamps of his design at the World's Columbian Exposition in Chicago.
- **1894**: Hutin & LeBlanc, espouse long held view that inductive energy transfer should be possible, they received U.S. Patent # 527,857 describing a system for power transfer at 3 kHz.
- **1894**: Tesla wirelessly lights up phosphorescent and incandescent lamps at the 35 South Fifth Avenue laboratory, and later at the 46 E. Houston Street laboratory in New York City by means of "electro-dynamic induction," that is to say wireless resonant inductive coupling.
- **1894**: Jagdish Chandra Bose ignites gunpowder and rings a bell at a distance using electromagnetic waves, showing that communications signals can be sent without using wires.
- **1895**: Bose transmits signals over a distance of nearly a mile.
- **1896**: Tesla transmits signals over a distance of about 48 kilometres (30 mi).
- **1897**: Guglielmo Marconi uses a radio transmitter to transmit Morse code signals over a distance of about 6 km.
- **1897**: Tesla files the first of his patent applications dealing specifically with wireless transmission.
- **1899**: In Colorado Springs, Tesla writes, "the inferiority of the induction method would appear immense as compared with the *disturbed charge of ground and air method*."
- **1900**: Marconi fails to get a patent for radio in the United States.
- **1901**: Marconi transmits signals across the Atlantic.
- **1902**: Tesla vs. Reginald Fessenden - U.S. Patent Interference No. 21,701, System of Signaling (wireless); selective illumination of incandescent lamps, time and

frequency domain spread spectrum telecommunications, electronic logic gates in general.

- **1904**: At the St. Louis World's Fair, a prize is offered for a successful attempt to drive a 0.1 horsepower (75 W) airship motor by energy transmitted through space at a distance of least 100 feet (30 m).
- **1916**: Tesla states, "In my [*disturbed charge of ground and air*] system, you should free yourself of the idea that there is [electromagnetic] radiation, that energy is radiated. It is not radiated; it is conserved."
- **1917**: Tesla's Wardenclyffe tower is demolished.
- **1926**: Shintaro Uda and Hidetsugu Yagi publish their first paper on Uda's *"tuned high-gain directional array"* better known as the Yagi antenna.
- **1961**: William C. Brown publishes an article exploring possibilities of microwave power transmission.
- **1964**: Brown demonstrates on CBS News with Walter Cronkite a model helicopter that received all the power needed for flight from a microwave beam. Between 1969 and 1975, Brown was technical director of a JPL Raytheon program that beamed 30 kW over a distance of 1 mile at 84% efficiency.
- **1968**: Peter Glaser proposes wirelessly transferring solar energy captured in space using "Powerbeaming" technology. This is usually recognized as the first description of a solar power satellite.
- **1971**: Prof. Don Otto develops a small trolley powered by induction at The University of Auckland, in New Zealand.
- **1973**: World first passive RFID system demonstrated at Los-Alamos National Lab.
- **1975**: Goldstone Deep Space Communications Complex does experiments in the tens of kilowatts.
- **1988**: A power electronics group led by Prof. John Boys at The University of Auckland in New Zealand, develops an inverter using novel engineering materials and power electronics and conclude that power transmission by means of electrodynamic induction should be achievable. A first prototype for a contact-less power supply is built. Auckland Uniservices, the commercial company of The University of Auckland, patents the technology.
- **1989**: Daifuku, a Japanese company, engages Auckland Uniservices Ltd. to develop technology for car assembly plants and materials handling providing challenging technical requirements including multiplicity of vehicles.
- **1990**: Prof. John Boys team develops novel technology enabling multiple vehicles to run on the same inductive power loop and provide independent control of each vehicle. Auckland UniServices Patents the technology.
- **1996**: Auckland Uniservices develops an Electric Bus power system using Electrodynamic Induction to charge (30-60 kW) opportunistically commencing implementation in New Zealand. Prof John Boys Team commission 1st commercial IPT Bus in the world at Whakarewarewa, in New Zealand.
- **1998**: RFID tags powered by electrodynamic induction over a few feet
- **1999**: Dr. Herbert L. Becker powers a lamp and a hand held fan from a distance of 30 feet.

- **2001**: Splashpower formed in the UK. Uses coupled resonant coils in a flat "pad" style to transfer tens of watts into a variety of consumer devices, including lamp, phone, PDA, iPod etc.
- **2004**: Electrodynamic Induction used by 90 percent of the US$1 billion clean room industry for materials handling equipment in semiconductor, LCD and plasma screen manufacture.
- **2005**: Prof Boys' team at The University of Auckland, refines 3-phase IPT Highway and pick-up systems allowing transfer of power to moving vehicles in the lab.
- **2007**: Using Electrodynamic Induction a physics research group, led by Prof. Marin Soljačić, at MIT, wirelessly power a 60W light bulb with 40% efficiency at a 2 metres (6.6 ft) distance with two 60 cm-diameter coils.
- **2008**: Bombardier offers new wireless transmission product PRIMOVE, a power system for use on trams and light-rail vehicles.
- **2008**: Industrial designer Thanh Tran, at Brunel University made a wireless lamp incorporating a high efficiency 3W LED.
- **2008**: Intel reproduces Nikola Tesla's original 1894 implementation of Electrodynamic Induction and Prof. John Boys group's 1988 follow-up experiments by wirelessly powering a nearby light bulb with 75% efficiency.
- **2008**: Greg Leyh and Mike Kennan of the Nevada Lightning Laboratory publish a paper on Nikola Tesla's *disturbed charge of ground and air method* of wireless power transmission with circuit simulations and test results showing an efficiency greater than can be obtained using the Electrodynamic Induction method.
- **2009**: A Consortium of interested companies called the Wireless Power Consortium announce they are nearing completion for a new industry standard for low-power Inductive charging
- **2009**: Palm (now a division HP) launches the Palm Pre smartphone with the Palm Touchstone wireless charger.
- **2009**: An Ex approved Torch and Charger aimed at the offshore market is introduced. This product is developed by Wireless Power & Communication, a Norway based company.
- **2009**: A simple analytical electrical model of electrodynamic induction power transfer is proposed and applied to a wireless power transfer system for implantable devices.
- **2009**: Lasermotive uses diode laser to win $900k NASA prize in power beaming, breaking several world records in power and distance, by transmitting over a kilowatt more than several hundred meters.
- **2009**: Sony shows a wireless electrodynamic-induction powered TV set, 60 W over 50 cm
- **2010**: Haier Group debuts “the world's first” completely wireless LCD television at CES 2010 based on Prof. Marin Soljačić's follow-up research on Nikola Tesla's electrodynamic induction wireless energy transmission method and the Wireless Home Digital Interface (WHDI).
- **2010**: System On Chip (SoC) group in University of British Columbia developed an optimization tool for design of highly efficient wireless power transfer system

using multiple coils. The design was optimized for implantable application and power transfer efficiency of 82% was achieved.

Near field

Near field is wireless transmission techniques over distances comparable to, or a few times the diameter of the device(s), and up to around a quarter of the wavelengths used. Near field energy itself is non radiative, but some radiative losses will occur. In addition there are usually resistive losses. Near field transfer is usually magnetic (inductive), but electric (capacitive) energy transfer can also occur.

Induction

The action of an electrical transformer is the simplest instance of wireless energy transfer. The primary and secondary circuits of a transformer are not directly connected. The transfer of energy takes place by electromagnetic coupling through a process known as mutual induction. (An added benefit is the capability to step the primary voltage either up or down.) The battery charger of a mobile phone or the transformers on the street are examples of how this principle can be used. Induction cookers and many electric toothbrushes are also powered by this technique.

The main drawback to induction, however, is the short range. The receiver must be very close to the transmitter or induction unit in order to inductively couple with it.

Resonant energy transfer

Resonant energy transfer or **resonant inductive coupling** is the near field wireless transmission of energy between two coils that are highly resonant at the same frequency. The equipment to do this is sometimes called a **resonant or resonance transformer**. While many transformers employ resonance, this type has a high *Q* and is often air cored to avoid 'iron' losses. The coils may be present in a single piece of equipment or in separate pieces of equipment.

Resonant transfer works by making a coil *ring* with an oscillating current. This generates an oscillating magnetic field. Because the coil is highly resonant any energy placed in the coil dies away relatively slowly over very many cycles; but if a second coil is brought near to it, the coil can pick up most of the energy before it is lost, even if it is some distance away. The fields used are predominately non radiative, near field (sometimes called evanescent waves), as all hardware is kept within 1/4 wavelength distance, and thus they radiate little energy from the transmitter to infinity.

One of the applications of the resonant transformer is for the CCFL inverter. Another application of the resonant transformer is to couple between stages of a superheterodyne

receiver, where the selectivity of the receiver is provided by tuned transformers in the intermediate-frequency amplifiers. Resonant transformers such as the Tesla coil can generate very high voltages with or without arcing, and are able to provide much higher current than electrostatic high-voltage generation machines such as the Van de Graaff generator. Resonant energy transfer is the operating principle behind proposed short range wireless electricity systems such as WiTricity and systems that have already been deployed, such as some types of RFID tags and contactless smart cards.

These types of systems generate magnetic fields that are unlikely to cause health issues in humans.

Resonant coupling

Non-resonant coupled inductors, such as typical transformers, work on the principle of a primary coil generating a magnetic field and a secondary coil subtending as much as possible of that field so that the power passing though the secondary is as close as possible to that of the primary. This requirement that the field be covered by the secondary results in very short range and usually requires a magnetic core. Over greater distances the non-resonant induction method is highly inefficient and wastes the vast majority of the energy in resistive losses of the primary coil.

Using resonance can help efficiency dramatically. If resonant coupling is used, each coil is capacitively loaded so as to form a tuned LC circuit. If the primary and secondary coils are resonant at a common frequency, it turns out that significant power may be transmitted between the coils over a range of a few times the coil diameters at reasonable efficiency.

Energy transfer and efficiency

The general principle is that if a given amount of energy is placed into a primary coil which is capacitively loaded, the coil will 'ring', and form an oscillating magnetic field. The energy will transfer back and forth between the magnetic field in the inductor and the electric field across the capacitor at the resonant frequency. This oscillation will die away at a rate determined by the *Q* factor, mainly due to resistive and radiative losses. However, provided the secondary coil cuts enough of the field that it absorbs more energy than is lost in each cycle of the primary, then most of the energy can still be transferred.

The primary coil forms a series RLC circuit, and the *Q* factor for such a coil is:

$$Q = \frac{1}{R}\sqrt{\frac{L}{C}},$$

Because the *Q* factor can be very high, (experimentally around a thousand has been demonstrated with air cored coils) only a small percentage of the field has to be coupled

from one coil to the other to achieve high efficiency, even though the field dies quickly with distance from a coil, the primary and secondary can be several diameters apart.

Coupling coefficient

The coupling coefficient is the fraction of the flux of the primary that cuts the secondary coil, and is a function of the geometry of the system. The coupling coefficient is between 0 and 1.

Systems are said to be tightly coupled, loosely coupled, critically coupled or overcoupled. Tight coupling is when the coupling coefficient is around 1 as with conventional transformers. Overcoupling is when the secondary coil is close enough that it tends to collapse the primary's field, and critical coupling is when the transfer in the passband is optimal. Loose coupling is when the coils are distant from each other, so that most of the flux misses the secondary, in Tesla coils around 0.2 is used, and at greater distances, for example for wireless power transmission, it may be lower than 0.01.

Power transfer

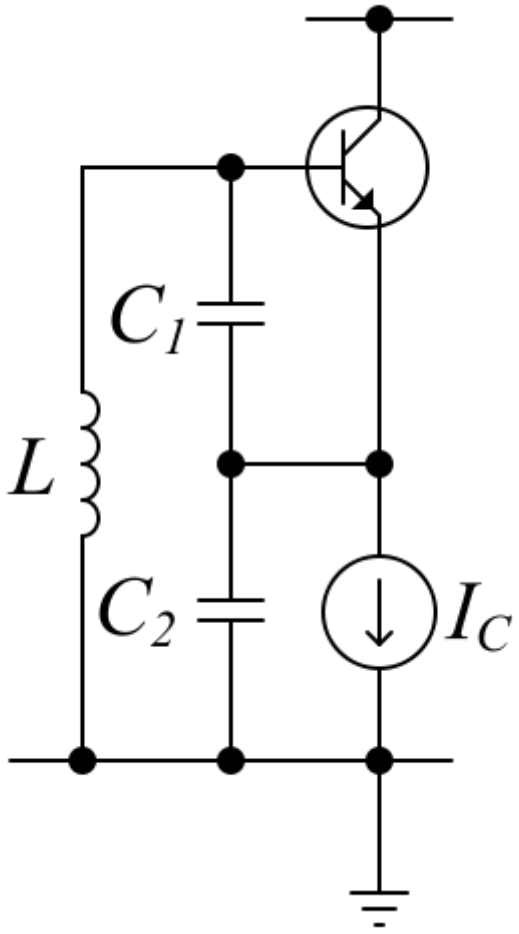
Because the Q can be very high, even when low power is fed into the transmitter coil, a relatively intense field builds up over multiple cycles, which increases the power that can be received—at resonance far more power is in the oscillating field than is being fed into the coil, and the receiver coil receives a percentage of that.

Voltage gain

The voltage gain of resonantly coupled coils is proportional to the square root of the ratio of secondary and primary inductances.

Transmitter coils and circuitry

Unlike the multiple-layer secondary of a non-resonant transformer, coils for this purpose are often single layer solenoids (to minimise skin effect and give improved Q) in parallel with a suitable capacitor, or they may be other shapes such as wave-wound litz wire. Insulation is either absent, with spacers, or low permittivity, low loss materials such as silk to minimise dielectric losses.

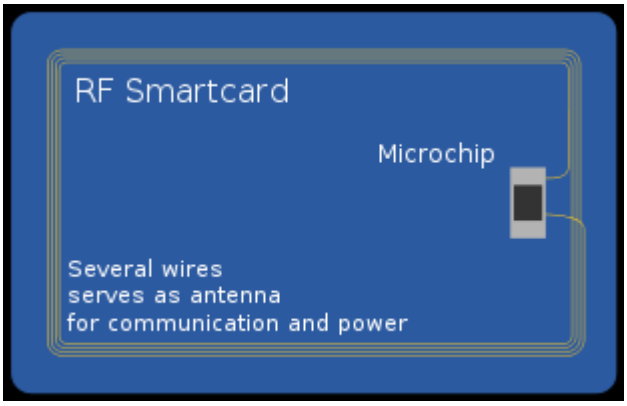


Colpitts oscillator. In resonant energy transfer the inductor would be the transmitter coil and capacitors are used to tune the circuit to a suitable frequency.

To progressively feed energy/power into the primary coil with each cycle, different circuits can be used. One circuit employs a Colpitts oscillator.

In Tesla coils an intermittent switching system, a "circuit controller or "break," is used to inject an impulsive signal into the primary coil; the secondary coil then rings and decays.

Receiver coils and circuitry

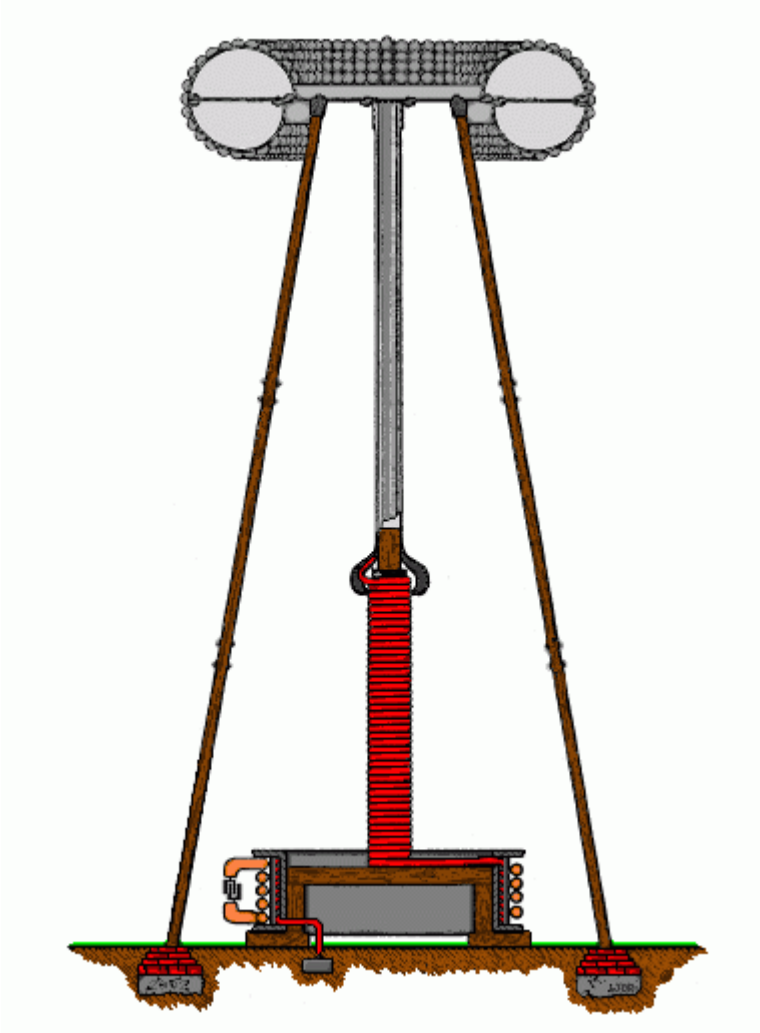


The receiver of a smart card has a coil connected to a chip which provides capacitance to give resonance as well as regulators to provided a suitable voltage

The secondary receiver coils are similar designs to the primary sending coils. Running the secondary at the same resonant frequency as the primary ensures that the secondary has a low impedance at the transmitter's frequency and that the energy is optimally absorbed.

To remove energy from the secondary coil, different methods can be used, the AC can be used directly or rectified and a regulator circuit can be used to generate DC voltage.

History



This advanced Tesla coil was designed to implement wireless energy transfer by means of the *disturbed charge of ground and air method.*

In 1894 Nikola Tesla used resonant inductive coupling, also known as "electro-dynamic induction" to wirelessly light up phosphorescent and incandescent lamps at the 35 South Fifth Avenue laboratory, and later at the 46 E. Houston Street laboratory in New York City.]]. In 1897 he patented a device called the high-voltage, resonance transformer or "Tesla coil." Transferring electrical energy from the primary coil to the secondary coil by resonant induction, a Tesla coil is capable of producing very high voltages at high frequency. The improved design allowed for the safe production and utilization of high-potential electrical currents, "without serioius liability of the destruction of the apparatus itself and danger to persons approaching or handling it."

In the early 1960s resonant inductive wireless energy transfer was used successfully in implantable medical devices including such devices as pacemakers and artificial hearts.

While the early systems used a resonant receiver coil, later systems implemented resonant transmitter coils as well. These medical devices are designed for high efficiency using low power electronics while efficiently accommodating some misalignment and dynamic twisting of the coils. The separation between the coils in implantable applications is commonly less than 20 cm. Today resonant inductive energy transfer is regularly used for providing electric power in many commercially available medical implantable devices.

Wireless electric energy transfer for experimentally powering electric automobiles and buses is a higher power application (>10 kW) of resonant inductive energy transfer. High power levels are required for rapid recharging and high energy transfer efficiency is required both for operational economy and to avoid negative environmental impact of the system. An experimental electrified roadway test track built circa 1990 achieved 80% energy efficiency while recharging the battery of a prototype bus at a specially equipped bus stop. The bus could be outfitted with a retractable receiving coil for greater coil clearance when moving. The gap between the transmit and receive coils was designed to be less than 10 cm when powered. In addition to buses the use of wireless transfer has been investigated for recharging electric automobiles in parking spots and garages as well.

Some of these wireless resonant inductive devices operate at low milliwatt power levels and are battery powered. Others operate at higher kilowatt power levels. Current implantable medical and road electrification device designs achieve more than 75% transfer efficiency at an operating distance between the transmit and receive coils of less than 10 cm.

In 1995, Professor John Boys and Prof Grant Covic, of The University of Auckland in New Zealand, developed systems to transfer large amounts of energy across small air gaps.

In 1998, RFID tags were patented that were powered in this way.

In November 2006, Marin Soljačić and other researchers at the Massachusetts Institute of Technology applied this near field behavior, well known in electromagnetic theory, the wireless power transmission concept based on strongly-coupled resonators. In a theoretical analysis, they demonstrate that, by designing electromagnetic resonators that suffer minimal loss due to radiation and absorption and have a near field with mid-range extent (namely a few times the resonator size), mid-range efficient wireless energy-transfer is possible. The reason is that, if two such resonant circuits tuned to the same frequency are within a fraction of a wavelength, their near fields (consisting of 'evanescent waves') couple by means of evanescent wave coupling (which is related to quantum tunneling). Oscillating waves develop between the inductors, which can allow the energy to transfer from one object to the other within times much shorter than all loss times, which were designed to be long, and thus with the maximum possible energy-transfer efficiency. Since the resonant wavelength is much larger than the resonators, the field can circumvent extraneous objects in the vicinity and thus this mid-range energy-

transfer scheme does not require line-of-sight. By utilizing in particular the magnetic field to achieve the coupling, this method can be safe, since magnetic fields interact weakly with living organisms.

Comparison with other technologies

Compared to inductive transfer in conventional transformers, except when the coils are well within a diameter of each other, the efficiency is somewhat lower (around 80% at short range) whereas tightly coupled conventional transformers may achieve greater efficiency (around 90-95%) and for this reason it cannot be used where high energy transfer is required at greater distances.

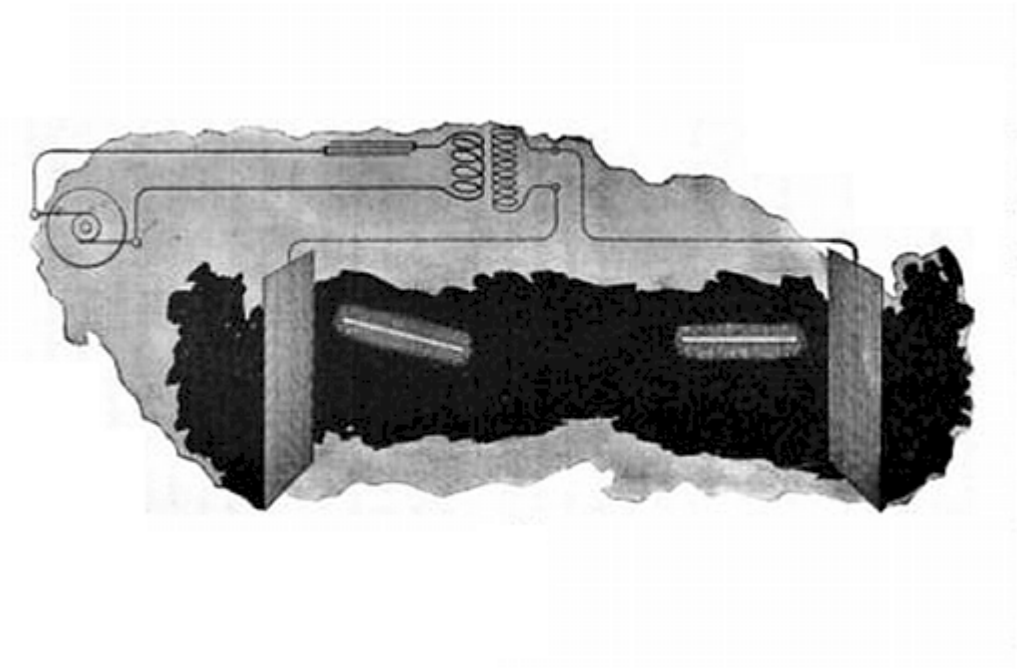
However, compared to the costs associated with batteries, particularly non-rechargeable batteries, the costs of the batteries are hundreds of times higher. In situations where a source of power is available nearby, it can be a cheaper solution. In addition, whereas batteries need periodic maintenance and replacement, resonant energy transfer could be used instead. Batteries additionally generate pollution during their construction and their disposal which largely would be avoided.

Regulations and safety

Unlike mains-wired equipment, no direct electrical connection is needed and hence equipment can be sealed to minimize the possibility of electric shock.

Because the coupling is achieved using predominantly magnetic fields; the technology may be relatively safe. Safety standards and guidelines do exist in most countries for electromagnetic field exposures (e.g.) Whether the system can meet the guidelines or the less stringent legal requirements depends on the delivered power and range from the transmitter.

Electrostatic induction



Tesla illuminating two exhausted tubes by means of a powerful, rapidly alternating electrostatic field created between two vertical metal sheets suspended from the ceiling on insulating cords.

The "electrostatic induction effect" or "capacitive coupling" is an electric field gradient or differential capacitance between two elevated electrodes over a conducting ground plane for wireless energy transmission involving high frequency alternating current potential differences transmitted between two plates or nodes. The electrostatic forces through natural media across a conductor situated in the changing magnetic flux can transfer energy to a receiving device (such as Tesla's wireless bulbs). Sometimes called "the Tesla effect" it is the application of a type of electrical displacement, i.e., the passage of electrical energy through space and matter, other than and in addition to the development of a potential across a conductor.

Tesla stated,

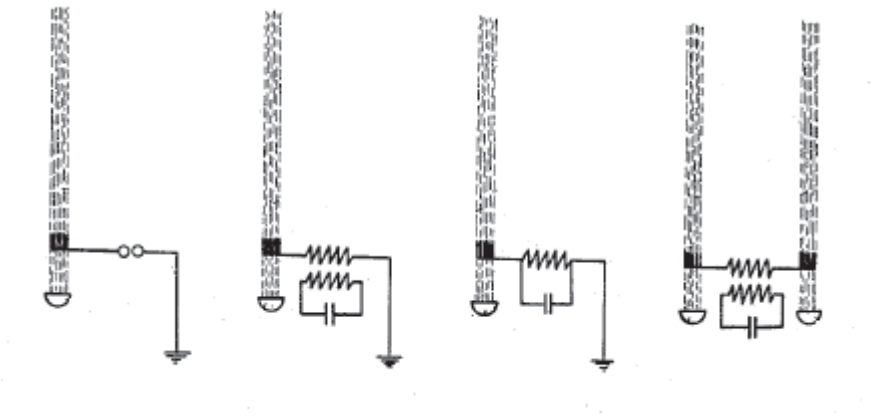
"Instead of depending on [electrodynamic] induction at a distance to light the tube . . . [the] ideal way of lighting a hall or room would . . . be to produce such a condition in it that an illuminating device could be moved and put anywhere, and that it is lighted, no matter where it is put and without being electrically connected to anything. I have been able to produce such a condition by creating in the room a powerful, ***rapidly alternating electrostatic field***. For this purpose I suspend a sheet of metal a distance from the ceiling on insulating cords and connect it to one terminal of the induction coil, the other terminal being preferably connected to the ground. Or else I suspend two sheets . . . each sheet being connected with one of the terminals of the coil, and their size being carefully

determined. An exhausted tube may then be carried in the hand anywhere between the sheets or placed anywhere, even a certain distance beyond them; it remains always luminous."

and

“In some cases when small amounts of energy are required the high elevation of the terminals, and more particularly of the receiving-terminal D' may not be necessary, since, especially when the frequency of the currents is very high, a sufficient amount of energy may be collected at that terminal by ***electrostatic induction*** from the upper air strata, which are rendered conducting by the active terminal of the transmitter or through which the currents from the same are conveyed."

Far field



Means for long conductors of electricity forming part of an electric circuit and electrically connecting said ionized beam to an electric circuit. Hettinger 1917 -(U.S. Patent 1,309,031)

Far field methods achieve longer ranges, often multiple kilometer ranges, where the distance is much greater than the diameter of the device(s). The main reason for longer ranges with radio wave and optical devices is the fact that electromagnetic radiation in the far-field can be made to match the shape of the receiving area (using high directivity antennas or well-collimated Laser Beam) thereby delivering almost all emitted power at long ranges. The maximum directivity for antennas is physically limited by diffraction.

Beamed power, size, distance, and efficiency

The size of the components may be dictated by the distance from transmitter to receiver, the wavelength and the Rayleigh criterion or diffraction limit, used in standard radio frequency antenna design, which also applies to lasers. In addition to the Rayleigh criterion Airy's diffraction limit is also frequently used to determine an approximate spot size at an arbitrary distance from the aperture.

The Rayleigh criterion dictates that any radio wave, microwave or laser beam will spread and become weaker and diffuse over distance; the larger the transmitter antenna or laser aperture compared to the wavelength of radiation, the tighter the beam and the less it will spread as a function of distance (and vice versa). Smaller antennae also suffer from excessive losses due to side lobes. However, the concept of laser aperture considerably differs from an antenna. Typically, a laser aperture much larger than the wavelength induces multi-moded radiation and mostly collimators are used before emitted radiation couples into a fiber or into space.

Ultimately, beamwidth is physically determined by diffraction due to the dish size in relation to the wavelength of the electromagnetic radiation used to make the beam. Microwave power beaming can be more efficient than lasers, and is less prone to atmospheric attenuation caused by dust or water vapor losing atmosphere to vaporize the water in contact.

Then the power levels are calculated by combining the above parameters together, and adding in the gains and losses due to the antenna characteristics and the transparency and dispersion of the medium through which the radiation passes. That process is known as calculating a link budget.

Radio and microwave

The earliest work in the area of wireless transmission via radio waves (electromagnetic waves) was performed by Nikola Tesla but he did not publish his work immediately. Later on, Guglielmo Marconi used a radio transmission patent from Nikola Tesla and presented as his own. Nikola Tesla appealed and after many years of court battles The United States Supreme Court awarded the radio transmission and reception patent exclusively to Nikola Tesla.

Japanese researcher Hidetsugu Yagi also investigated wireless energy transmission using a directional array antenna that he designed. In February 1926, Yagi and Uda published their first paper on the tuned high-gain directional array now known as the Yagi antenna. While it did not prove to be particularly useful for power transmission, this beam antenna has been widely adopted throughout the broadcasting and wireless telecommunications industries due to its excellent performance characteristics.

Power transmission via radio waves can be made more directional, allowing longer distance power beaming, with shorter wavelengths of electromagnetic radiation, typically in the microwave range. A rectenna may be used to convert the microwave energy back into electricity. Rectenna conversion efficiencies exceeding 95% have been realized. Power beaming using microwaves has been proposed for the transmission of energy from orbiting solar power satellites to Earth and the beaming of power to spacecraft leaving orbit has been considered.

Power beaming by microwaves has the difficulty that for most space applications the required aperture sizes are very large due to diffraction limiting antenna directionality.

For example, the 1978 NASA Study of solar power satellites required a 1-km diameter transmitting antenna, and a 10 km diameter receiving rectenna, for a microwave beam at 2.45 GHz. These sizes can be somewhat decreased by using shorter wavelengths, although short wavelengths may have difficulties with atmospheric absorption and beam blockage by rain or water droplets. Because of the Thinned array curse, it is not possible to make a narrower beam by combining the beams of several smaller satellites.

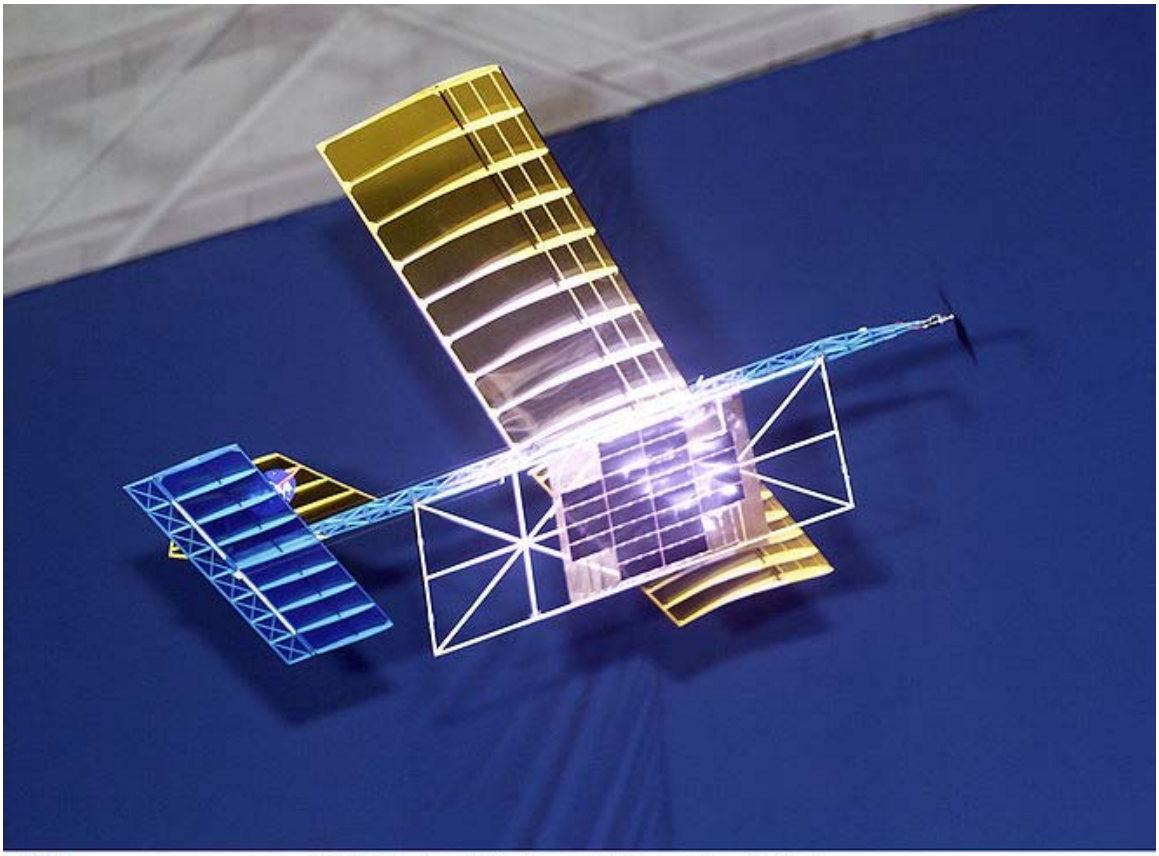
For earthbound applications a large area 10 km diameter receiving array allows large total power levels to be used while operating at the low power density suggested for human electromagnetic exposure safety. A human safe power density of 1 mW/cm^2 distributed across a 10 km diameter area corresponds to 750 megawatts total power level. This is the power level found in many modern electric power plants.

High power

Wireless Power Transmission (using microwaves) is well proven. Experiments in the tens of kilowatts have been performed at Goldstone in California in 1975 and more recently (1997) at Grand Bassin on Reunion Island.

These methods achieve distances on the order of a kilometer.

Laser



NASA Dryden Flight Research Center Photo Collection
http://www.dfrc.nasa.gov/Gallery/Photo/index.html
NASA Photo: ED03-0249-18 Date: September 18, 2003 Photo By: Tom Tschida

With a laser beam centered on its panel of photovoltaic cells, a model plane makes the first flight of an aircraft powered by a laser beam inside a building at NASA Marshall.

With a laser beam centered on its panel of photovoltaic cells, a lightweight model plane makes the first flight of an aircraft powered by a laser beam inside a building at NASA Marshall Space Flight Center.

In the case of electromagnetic radiation closer to visible region of spectrum (10s of microns (um) to 10s of nm), power can be transmitted by converting electricity into a laser beam that is then pointed at a solar cell receiver. This mechanism is generally known as "powerbeaming" because the power is beamed at a receiver that can convert it to usable electrical energy.

There are quite a few unique advantages of laser based energy transfer that outweigh the disadvantages.

1. collimated monochromatic wavefront propagation allows narrow beam cross-section area for energy confinement over large ranges.

2. compact size of solid state lasers-photovoltaics semiconductor diodes allows ease of integration into products with small form factors.
3. ability to operate with zero radio-frequency interference to existing communication devices i.e. wi-fi and cell phones.
4. control of Wireless Energy Access, instead of omnidirectional transfer where there can be no authentication before transferring energy.

These allow laser-based wireless energy transfer concept to compete with conventional energy transfer methods.

Its drawbacks are:

1. Conversion to light, such as with a laser, is moderately inefficient (although quantum cascade lasers improve this)
2. Conversion back into electricity is moderately inefficient, with photovoltaic cells achieving 40%-50% efficiency. (Note that conversion efficiency is rather higher with monochromatic light than with insolation of solar panels).
3. Atmospheric absorption causes losses.
4. As with microwave beaming, this method requires a direct line of sight with the target.

The laser "powerbeaming" technology has been mostly explored in military weapons and aerospace applications and is now being developed for commercial and consumer electronics Low-Power applications. Wireless energy transfer system using laser for consumer space has to satisfy Laser safety requirements standardized under IEC 60825.

To develop an understanding of the trade-offs of Laser ("a special type of light wave"-based system):

1. Propagation of a laser beam (on how Laser beam propagation is much less affected by diffraction limits)
2. Coherence and the range limitation problem (on how spatial and spectral coherence characteristics of Lasers allows better distance-to-power capabilities)
3. Airy disk (on how wavelength fundamentally dictates the size of a disk with distance)
4. Applications of laser diodes (on how the laser sources are utilized in various industries and their sizes are reducing for better integration)

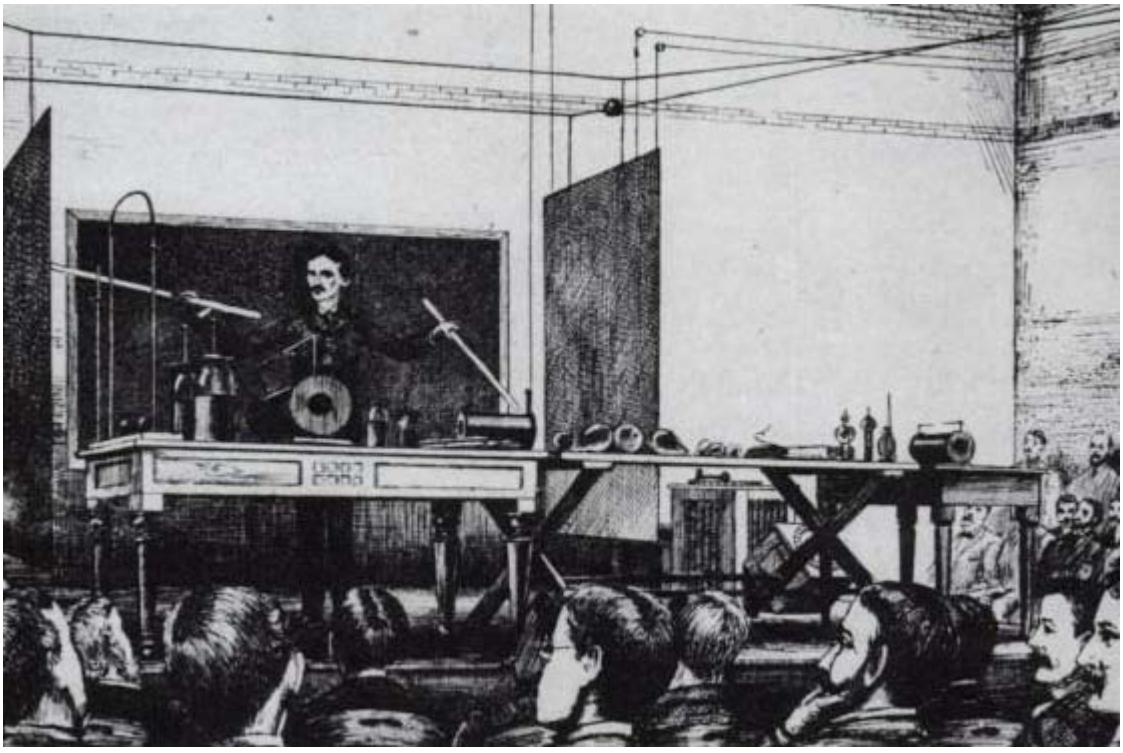
Geoffrey Landis is one of the pioneers of solar power satellite and laser-based transfer of energy especially for space and lunar missions. The continuously increasing demand for safe and frequent space missions has resulted in serious thoughts on a futuristic space elevator that would be powered by lasers. NASA's space elevator would need wireless power to be beamed to it for it to climb a tether.

NASA's Dryden Flight Research Center has demonstrated flight of a lightweight unmanned model plane powered by a laser beam. This proof-of-concept demonstrates the

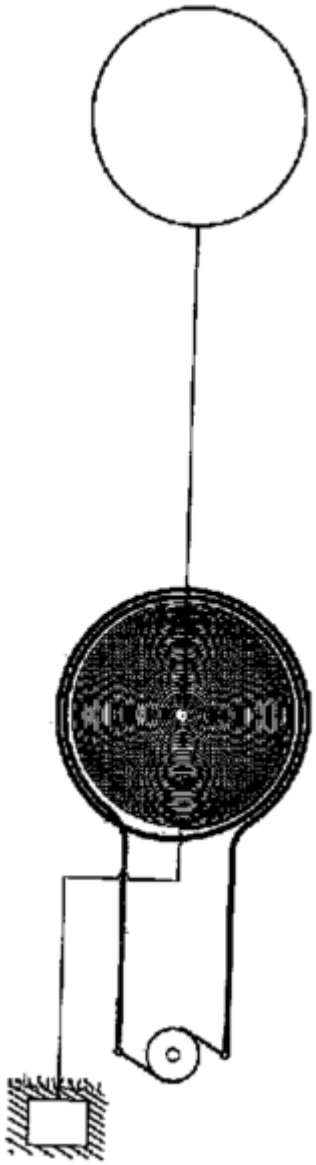
feasibility of periodic recharging using the laser beam system and the lack of need to return to ground.

"Lasermotive" demonstrated laser powerbeaming at one kilometer during NASA's 2009 powerbeaming contest. Also "Lighthouse DEV" (a spin off of NASA Power Beaming Team) along with "University of Maryland" is developing an eye safe laser system to power an small UAV. Since 2006, "PowerBeam" which originally invented the eye-safe technology and holds all crucial patents in this technology space, is developing commercially ready units for various consumer and industrial electronic products.

Electrical conduction



Wireless energy transmission demonstration during Tesla's high frequency and potential lecture of 1891.



Tesla coil transformer wound in the form of a flat spiral. This is the transmitter form as described in U.S. Patent 645,576.

Electrical energy can be transmitted by means of electrical currents made to flow through naturally existing conductors, specifically the earth, lakes and oceans, and through the upper atmosphere starting at approximately 35,000 feet (11,000 m) elevation — a natural medium that can be made conducting if the breakdown voltage is exceeded and the constituent gas becomes ionized. For example, when a high voltage is applied across a neon tube the gas becomes ionized and a current passes between the two internal electrodes. In a wireless energy transmission system using this principle, a high-power ultraviolet beam might be used to form vertical ionized channels in the air directly above the transmitter-receiver stations. The same concept is used in virtual lightning rods, the electrolaser electroshock weapon and has been proposed for disabling vehicles. A global

system for "the transmission of electrical energy without wires" dependant upon the high electrical conductivity of the earth was proposed by Nikola Tesla as early as 1904.

"The earth is 4,000 miles radius. Around this conducting earth is an atmosphere. The earth is a conductor; the atmosphere above is a conductor, only there is a little stratum between the conducting atmosphere and the conducting earth which is insulating. . . . Now, you realize right away that if you set up differences of potential at one point, say, you will create in the media corresponding fluctuations of potential. But, since the distance from the earth's surface to the conducting atmosphere is minute, as compared with the distance of the receiver at 4,000 miles, say, you can readily see that the energy cannot travel along this curve and get there, but will be immediately transformed into conduction currents, and these currents will travel like currents over a wire with a return. The energy will be recovered in the circuit, not by a beam that passes along this curve and is reflected and absorbed, . . . but it will travel by conduction and will be recovered in this way."

Researchers experimenting with Tesla's wireless energy transmission system design have made observations that may be inconsistent with a basic tenet of physics related to the scalar derivatives of the electromagnetic potentials, which are presently considered to be *nonphysical*.

The intention of the Tesla world wireless energy transmission system is to combine electrical power transmission along with broadcasting and point-to-point wireless telecommunications, and allow for the elimination of many existing high-tension power transmission lines, facilitating the interconnection of electrical generation plants on a global scale.

One of Tesla's patents suggests he may have misinterpreted 25–70 km nodal structures associated with cloud-ground lightning observations made during the 1899 Colorado Springs experiments in terms of circumglobally propagating standing waves instead of a local interference phenomenon of direct and reflected waves.

Regarding the recent notion of power transmission through the earth-ionosphere cavity, a consideration of the earth-ionosphere or concentric spherical shell waveguide propagation parameters as they are known today shows that wireless energy transfer by ***direct*** excitation of a Schumann cavity resonance mode is not realizable. "The conceptual difficulty with this model is that, at the very low frequencies that Tesla said that he employed (1-50 kHz), earth-ionosphere waveguide excitation, now well understood, would seem to be impossible with the either the Colorado Springs or the Long Island apparatus (at least with the apparatus that is visible in the photographs of these facilities)."

On the other hand, Tesla's concept of a global wireless electrical power transmission grid and telecommunications network based upon energy transmission by means of a spherical conductor transmission line with an upper three-space model return circuit, while perhaps not practical for power transmission, is feasible, defying no law of physics.

Global wireless energy transmission by means of a spherical conductor "single-wire" surface wave transmission line and a propagating TM_{00} mode may also be possible, a feasibility study using a sufficiently powerful and properly tuned Tesla coil earth-resonance transmitter being called for.

Tesla patents

Nikola Tesla had multiple patents disclosing long distance wireless transmission. U.S. Patent 0,645,576 *System of Transmission of Electrical Energy* and U.S. Patent 0,649,621 *Apparatus for Transmission of Electrical Energy*, describe useful combinations of transformer coils for this purpose. The transmitter is arranged and excited to cause electrical energy to propagate through the natural medium from one point to another remote point to a receiver of the transmitted signals. The production of currents at very high potential is attained in these oscillators. U.S. Patent 0,787,412 *Art of Transmitting Electrical Energy through the Natural Mediums* describes a combined system for broadcasting, point-to-point wireless telecommunications and electrical power distribution achieved through the use of earth-resonance principles.