Networks and Telecommunication

Assignment

R. C. A. Wijeratne
07/AS/CI/032
EP594

WI-Fi Technology

Introduction

Wi-Fi is a mechanism for wirelessly connecting electronic devices. A device enabled with Wi-Fi, such as a personal computer, video game console, smartphone, or digital audio player, can connect to the Internet via a wireless network access point. An access point (or hotspot) has a range of about 20 meters (65 ft) indoors and a greater range outdoors. Multiple overlapping access points can cover large areas. "Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards. Wi-Fi is used by over 700 million people. There are over four million hotspots (places with Wi-Fi Internet connectivity) around the world, and about 800 million new Wi-Fi devices are sold every year. Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" designation and trademark.

Uses

To connect to a Wi-Fi LAN, a computer has to be equipped with a wireless network interface controller. The combination of computer and interface controller is called a station. All stations share a single radio frequency communication channel. Transmissions on this channel are received by all stations within range. The hardware does not signal the user that the transmission was delivered and is therefore called a best-effort delivery mechanism. A carrier wave is used to transmit the data in packets, referred to as "Ethernet frames". Each station is constantly tuned in on the radio frequency communication channel to pick up available transmissions.

Internet access

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 — comprises 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 successfully in wireless mesh networks in London, UK, for example.

Wi-Fi provides service in private homes and offices as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially. Organizations and businesses, such as 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 city-wide Wi-Fi (Muni-Fi) projects had been created. 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 buildings, provide Internet access and internetworking to all devices tuned into them, wirelessly or via cable. 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 iPhone, Android, Bada and Symbian phones can create wireless connections.

One can also connect Wi-Fi devices in ad-hoc mode for client-to-client connections without a router. Wi-Fi also connects places normally without network access, such as kitchens and garden sheds.

City-wide Wi-Fi

In the early 2000s, many cities around the world announced plans to construct city-wide Wi-Fi networks. Doing so proved to be more difficult than envisioned, and as a result most of these projects were either cancelled or placed on indefinite hold. A few were successful; for example, in 2005 Sunnyvale, California, became the first city in the United States to offer city-wide free Wi-Fi, and Minneapolis has generated $1.2 million in profit annually for its provider.

In May 2010, London, UK, Mayor Boris Johnson pledged to have London-wide Wi-Fi by 2012. Both London and Islington in the UK already have extensive outdoor Wi-Fi coverage.

In 2010 Mysore became India's first Wi-fi-enabled city and second in the world after Jerusalem. A company called WiFiyNet has set up hotspots in Mysore, covering the complete city and a few nearbly villages.

Advantages

Wi-Fi allows cheaper deployment of local area networks (LANs). Also spaces where cables cannot be run, such as outdoor areas and historical buildings, can host wireless LANs.

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.

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. 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 widely 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 are not consistent worldwide: most of Europe allows for an additional two channels beyond those permitted in the U.S. for the 2.4 GHz band (1–13 vs. 1–11), while Japan has one more on top of that (1–14). Europe, as of 2007, was essentially homogeneous in this respect.

A Wi-Fi signal occupies five channels in the 2.4 GHz band; any two channels whose channel numbers differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate; channels 1, 6, and 11 do, however, comprise the only group of three non-overlapping channels in the U.S.

The current 'fastest' norm, 802.11n, uses double the radio spectrum compared to 802.11a or 802.11g. This means there can only be one 802.11n network on 2.4 GHz band without interference to other WLAN traffic.

The Internet protocol was designed for a wired network in which packet loss due to noise is very rare and packets are lost almost exclusively due to congestion. On a wireless network, noise is common. This difference causes TCP to greatly slow or break transmission when noise is significant, even when most packets are still arriving correctly.

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 VPN or secure Hypertext Transfer Protocol (HTTPS) over Transport Layer Security.