D. Trapeznikov
Group 25RPh112
Tyumen State University
Institute of Physics and Chemistry
A. Yusupova
Tyumen State University
Department of Foreign languages and
Intercultural Professional Communication of Science
Senior Lecturer
Д.В. Трапезников
студент группы 25РФ112
Тюменский государственный университет ИФиХ
А.А. Юсупова
Тюменский государственный университет
Кафедра иностранных языков и
межкультурной профессиональной коммуникации
естественнонаучных направлений
старший преподаватель

WI-FI NETWORK

БЕСПРОВОДНАЯ СЕТЬ WI-FI

1. Wi-Fi

1.1. The term Wi-Fi

The term Wi-Fi suggests Wireless Fidelity, resembling the long-established audio-equipment classification term Hi-Fi or high fidelity.

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'".

In fact Interbrand invented Wi-Fi as a play on words with Hi-Fi, and also created the 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.

Wi-Fi, is a mechanism that allows an electronic device to exchange data wirelessly over a computer network. A device enabled with Wi-Fi, such as a personal computer, video game console, smartphone, tablet, or digital audio player, can connect to a network resource such as the Internet via a wireless network access point (or hotspot).

"Wi-Fi" is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE(Institute of Electrical and Electronics Engineers) 802.11 family of standards. Only Wi-Fi products that complete Wi-Fi Alliance interoperability certification testing successfully may use the "Wi-Fi CERTIFIED" designation and trademark.

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN Standards Committee (IEEE 802). The base version of the standard IEEE 802.11-2007 has had subsequent amendments. These standards provide the basis for wireless network products using the Wi-Fi brand.

1.2. History

802.11 technology has its origins in a 1985 ruling by the US Federal Communications Commission that released the ISM band for unlicensed use. In 1991 NCR Corporation with AT&T invented the precursor to 802.11 intended for use in cashier systems. The first wireless products were under the name WaveLAN.

Vic Hayes has been called the "father of Wi-Fi". He was involved in designing the initial standards within the IEEE.

In 1992 and 1996, Australian organization the CSIRO obtained patents for a method later used in Wi-Fi to "unsmear" the signal. In April 2009, 14 tech companies agreed to pay CSIRO for infringements on the CSIRO patents. This lead to WiFi being attributed as an Australian invention.

The non-profit Wi-Fi Alliance formed in 1999 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.

1.3. 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.

1.4. Internet access

A Wi-Fi-enabled device 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. Outdoor public Wi-Fi technology has been used successfully in wireless mesh networks in London, UK.

Wi-Fi Alliance provides service in private homes, high street chains and independent businesses, 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 customers

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.

One can also connect Wi-Fi devices in ad-hoc mode for client-to-client connections without a router.

1.5. Wi-Fi certification

The Wi-Fi Alliance enforces the use of the Wi-Fi brand to technologies based on the IEEE 802.11 standards. This includes wireless local area network (WLAN) connections, device to device connectivity [such as Wi-Fi Peer to Peer], Personal area network (PAN), local area network (LAN) and even some limited wide area network (WAN) connections.

Not every Wi-Fi device is submitted for certification. The lack of Wi-Fi certification does not necessarily imply a device is incompatible with other Wi-Fi devices. If it is compliant or partly compatible, the Wi-Fi Alliance may not object to its description as a Wi-Fi device though technically only certified devices are approved.

The IEEE does not test equipment for compliance with their standards. 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.

2. Advantages and problems

2.1. 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.[citation needed]

Unlike mobile phones, any standard Wi-Fi device will work anywhere in the world.

2.2. Limitations

Spectrum assignments and operational limitations are not consistent worldwide: most of Europe allows for an additional two channels beyond those permitted in the US for the 2.4 GHz band (1–13 vs. 1–11), while Japan has one more on top of that (1–14).

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

Equivalent isotropically radiated power (EIRP) in the EU is limited to 20 dBm (100 mW).

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.

2.3. Range

Wi-Fi networks have limited range. A typical wireless access point using 802.11b or 802.11g with a stock antenna might have a range of 32 m (120 ft) indoors and 95 m (300 ft) outdoors. IEEE 802.11n, however, can exceed that range by more than two times. Range also varies with frequency band. Wi-Fi in the 2.4 GHz frequency block has slightly better range than Wi-Fi in the 5 GHz frequency block which is used by 802.11a. On wireless routers with detachable antennas, it is possible to improve range by fitting upgraded antennas which have

higher gain in particular directions. Outdoor ranges can be improved to many kilometers through the use of high gain directional antennas at the router and remote device(s).

Due to reach requirements for wireless LAN applications, Wi-Fi has fairly high power consumption compared to some other standards. Technologies such as Bluetooth provide a much shorter propagationrange of <10m[38] and so in general have a lower power consumption. Other low-power technologies such as ZigBee have fairly long range, but much lower data rate. The high power consumption of Wi-Fi makes battery life in mobile devices a concern.

Researchers have developed a number of "no new wires" technologies to provide alternatives to Wi-Fi for applications in which Wi-Fi's indoor range is not adequate and where installing new wires is not possible or cost-effective. For example, the ITU-T G.hn standard for high speed Local area networks uses existing home wiring (coaxial cables, phone lines and power lines). Although G.hn does not provide some of the advantages of Wi-Fi (such as mobility or outdoor use), it's designed for applications (such as IPTV distribution) where indoor range is more important than mobility.

Due to the complex nature of radio propagation at typical Wi-Fi frequencies, particularly the effects of signal reflection off trees and buildings, algorithms can only approximately predict Wi-Fi signal strength for any given area in relation to a transmitter.This effect does not apply equally to long-range Wi-Fi, since longer links typically operate from towers that transmit above the surrounding foliage.

The practical range of Wi-Fi essentially confines mobile use to such applications as inventory-taking machines in warehouses or in retail spaces. 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. Other wireless technologies are more suitable for communicating with moving vehicles.

2.4. Interferences

Wi-Fi connections can be disrupted or the internet speed lowered by having other devices in the same area. 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. Wi-Fi pollution, or an excessive number of access points in the area, especially on the 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 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, cordless phones 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.

2.5. Standard devices

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 etc. 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. 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, as is the case with as Apple's AirPort, which is managed with the AirPort Utility on Mac OS X and Microsoft Windows.

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.

2.6. Embedded systems

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 by OEMs so that implementers need only minimal Wi-Fi knowledge to provide Wi-Fi connectivity for their products.

2.7. Multiple access points

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 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.

2.8. 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.

2.9. 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 reduces security 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.

2.10. Securing methods

A common measure to deter unauthorized users involves hiding the access point's name by disabling the SSID broadcast. While effective against the casual user, it is ineffective as a security method because the SSID is broadcast in the clear in response to a client SSID query. Another method is to only allow computers with known MAC addresses to join the network, but determined eavesdroppers may be able join the network by spoofing an authorized address.

Wired Equivalent Privacy (WEP) encryption was designed to protect against casual snooping but it is no longer considered secure. Tools such as AirSnort or Aircrack-ng can quickly recover WEP encryption keys. Because of

WEP's weakness the Wi-Fi Alliance approved Wi-Fi Protected Access (WPA) which uses TKIP(Temporal Key Integrity Protocol). WPA was specifically designed to work with older equipment usually through a firmware upgrade. Though more secure than WEP, WPA has known vulnerabilities.

The more secure WPA2 using Advanced Encryption Standard was introduced in 2004 and is supported by most new Wi-Fi devices. WPA2 is fully compatible with WPA.

A flaw in a feature added to Wi-Fi in 2007, called Wi-Fi Protected Setup, allows WPA and WPA2 security to be bypassed and effectively broken in many situations. The only remedy as of late 2011 is to turn off Wi-Fi Protected Setup, which is not always possible.

2.11. 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.

Piggybacking often occurs unintentionally, since 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 (Man-in-the-middle attack). 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.

2.12. Health issues

A small percentage of Wi-Fi users have reported adverse health issues after repeat exposure and use of Wi-Fi, though there has been no publication of any effects being observable in double-blind studies. A review of studies involving 725 people that claimed electromagnetic hypersensitivity found no evidence for their claims. The ubiquity of Wi-Fi has led to calls for more research into the effects of "electronic smog".

The World Health Organization (WHO) says "there is no risk from low level, long-term exposure to wi-fi networks" and the United Kingdom's Health Protection Agency reports that exposure to Wi-Fi for a year results in "same amount of radiation from a 20-minute mobile phone call."

3. Conclusion

Relevance of the Wi-Fi technology is obvious. Nowadays, Wi-Fi is mainly used for making easy connections between a home computer and the Internet. But soon, we will see solutions for all kinds of wireless transmissions — including streaming of music and video. In addition, society’s need for information will be growing up. Therefore, this technology will be strongly developed.

REFERENCES:

1. A Technical Tutorial on the IEEE 802.11 Protocol. [Электронный ресурс]. – Режим доступа: http://www.citeulike.org.

2. Ross, John. The Book of Wi-Fi. [Электронный ресурс]. – Режим доступа: //http://www.ebooksdownloadfree.com.
3. Wikipedia. [Электронный ресурс]. – Режим доступа: http://en.wikipedia.org/wiki/Wi-Fi.