# Wi-Fi networks in small and medium-sized businesses (SMB)

**Mariusz Sojak[1], Szymon Głowacki[1]**
[1] Faculty of Production Engineering
Warsaw University of Life Sciences
ul. Nowoursynowska 166, 02-787 Warszawa, Poland
mariusz_sojak@sggw.pl

**Abstract.** Wi-Fi is quite a new technology on the market. This paper's aim was to prove the justifiability and profitability of this technology use in the small and medium-sized businesses sector. Advantages and disadvantages of this kind of network were also shown. An issue connected with data and configuration elements security was also raised. Other wireless technologies were also presented.

**Keywords:** Wi-Fi, wireless network, small and medium-sized business, IEEE 802.11, IEEE 802.15, IEEE 802.16 standard, WLAN

## 1 Introduction

The end of the 20th century is no doubt a period of systematic introduction of computers to various areas of our life. Computers are not only present in companies and enterprises but also in our homes. Fast and efficient communication is a key issue for companies. The connection used so far, based on wires, is the fastest one and provides high capacity transmission lines. However, in case of changing the location of a particular working place within a room or a building the cables providing access to the company's network, and, consequently, to the Internet, become an obstacle.

This is when a Wi-Fi (Wireless Fidelity) technology comes to our aid. Radio communication is used in WLANs (Wireless Local Area Networks), i.e. local networks that do not use wires. This paper focuses on the companies that belong to a small or medium-sized businesses (SMB) sector, i.e. employ 10-50 and to 250 employees respectively (ECC Decision, 2004).

SMB businesses play a significant role in the economies of states that belong to the European Union  including Poland, where SMB constitute about 99% of all the businesses. "Polish MSP employ a little over two thirds of the total number of people employed in the whole economy" (Journal SAP Poland No 2 (18/2004). SMB in Poland also include agricultural businesses.

## 2 Wireless technologies

The most popular commercial solutions among wireless computer network include: IrDA, Bluethooth, Wi-Fi, WiMAX. Each of these networks uses electromagnetic waves of different length. Thus, the main difference between these technologies is the possibility of using them depending on the distance between the transmitters and receivers. Whether there is no obstacle in the vision between the devices is also significant.

*IrDA (Infrared Data Association)* – data transmission system within infrared range, is mainly designed for creating Ad hoc networks, parts of which may be laptops, palmtops, printers, cameras, etc. Unfortunately, devices that use infrared are only able to interconnect using point-point connection (Zieliński 2000, pl.wikipedia.org, en.wikipedia.org, Wrocławski 2000). Conditions that must be met in order to establish connection are the visibility of the devices and the distance that does not exceed one metre. The angle of transmission beam is also limited to 30 °. Thanks to that a lot of IrDA connections may work next to each other without interferences. This standard is characterized by a simple and cheap implementation, small power consumption, efficient and stable data transfer and transmission speed: IrDA 1.0 = = 115kb/s , IrDA 1.1 = 4 Mb/s.

*Bluetooth* – this technology uses radio waves in the ISM (Industrial, Scientific, Medical) frequency band of 2.4GHz. Bluetooth divides the band it uses into 79 radio channels, 1 MHz each (range from 2402 to 2480 MHz). Data transmission speed of 1Mbit/s is obtained by using FSK (Frequency Shift Keying) modulation. Frequency hopping (1600 hops per second) makes it possible to assign the channels justly. An advantage of Bluetooth over IrDA is the possibility of creating a network, where more than two devices can communicate at the same time; the most frequent example being PAN (Personal Area Network). This standard allows to create point-multipoint networks (Zieliński 2000, Engst and Fleishman 2005, www.bluetooth.com). Data transmission range depends on the transmitter power, Table 2.1.

**Table 2.1.** Bluetooth range depending on the transmitter

| Class number | Transmitter power | Range | Notes |
|---|---|---|---|
| Class 1 | 100 mW | more than 100 m | - |
| Class 2 | 2.5 mW | 10 m | The most popular |
| Class 3 | 1 mW | up to 1 m | Rarely used |

In a network based on Bluetooth technology, there is a limitation, namely, master device can connect to a maximum number of 7 devices in the slave mode.

A network created in this way is called a Piconet. Piconets may connect with each other. However, the master device in one Piconet network cannot be the master device in another network of the same type. As a result of interconnection of two Piconet networks, one larger network, called Scatternet, is created, Figure 2.1. In order to create a Scatternet network, we most often use a bridge, which works in slave mode.

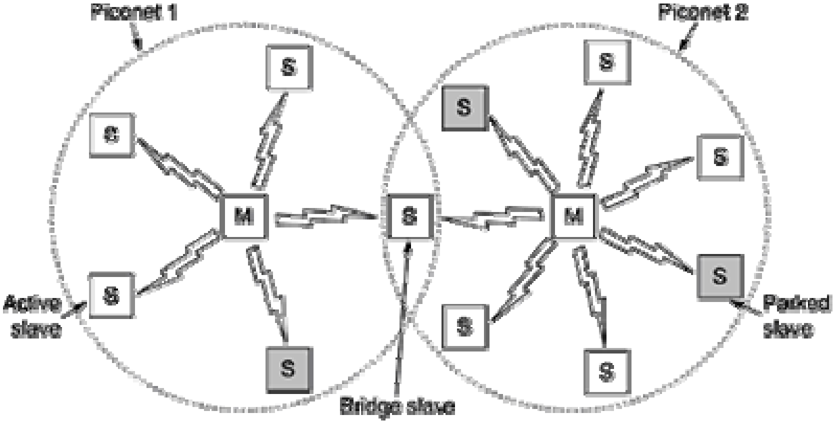

**Figure 2.1.** A scatternet network – two piconets connected together. (Source http://pl.wikipedia.org/wiki/Bluetooth)

This standard is characterized by an easy and cheap implementation, small power consumption, a possibility of establishing point-multipoint connections, efficient and stable data transfer and transmission speed of 3.0 Mb/s).

<u>*Wi-Fi (Wireless Fidelity*</u> – a set of standards used for creating wireless computer networks. Wi-Fi is a trademark that belongs to Wi-Fi Alliance. It is an association, which, at the time IEEE standards: 802.11, 802.11a, 802.11b appeared, coordinated and guided works to ensure communication compatibility between devices produced by different companies. Wi-Fi logo on devices ensures us that a given device is compatible with any device produced by another company on condition that it has the logo of this association. The only thing that must be must be considered is a standard, in which the device works, i.e. IEEE 802.11 and the letter defining a particular standard (Zieliński 2000, Ross 2005).

*WiMAX (World Interoperability for Microwave Access)* – this standard is also known as IEEE 802.16, it is IEEE 802.11. successor. Wi-Fi may be compared to a classical (cable) LAN network as regards the range, while WiMAX is a wireless WAN network. In 2001, first implementation of a far-range network came into public use. The frequency band, in which this technology can work is between 10 and 66 GHz, but due to the requirement of visibility between the devices the range was changed and is between 2 and 11 GHz. A new standard was described as 802.16b and 802.16c, and both of them came into use in 2003 (http://pl.wikipedia.org, http://en.wikipedia.org). The first non-commercial solution using WiMAX in Poland was the implementation of the network in a territorial unit Zielonka, near Warsaw in 2005.

## 3 Wi-Fi networks

802.11 wireless networks work in an allocated radio waves spectrum, with 2.4 GHz frequency, with the exception of 802.11a standard, which works in 5 GHz spectrum. In the majority of countries this spectrum is made available for public use and no licence is required. However, the devices used require certification. Since 1st May 2004, producers have been responsible for compatibility of the devices (CE mark). In Poland, a radio licence for a Wi-Fi device with the maximum emitted signal power of 100 mW is not required. The fact that a given frequency is not exclusive requires the devices to be exceptionally interference-proof. Despite a high resistance to interferences, they may still occur as a result of telephones, wireless camcorders, or microwave ovens (which emit 2.4 GHz waves) and are located near access points. Overlapping signals require the devices using wireless transmission to possess the ability to separate signals. Wireless devices use two methods of distinguishing overlapping signals, namely FHSS or DSSS.

*FHSS (Frequency Hopping Spread Spectrum)* – is a modulation in the spread spectrum with a hopping change of frequency channel, FH abbreviation is also used in literature. This method employs a very fast change of frequency channel, which is used for transmission.

2.4 GHz band was divided into 75 sub-channels, 1 MHz width each. Frequency change demands sending a data stream with an additional portion of information which makes FHSS transmission relatively slow. Hop technology across frequencies in the spread spectrum was developed by an actress Hedy Lamarr and an American composer George Antheil. The technology was called a system of confidential communication, as it was to be used for operating radio-controlled torpedoes resistant to enemy-generated interference. (Ross 2005).

*DSSS (Direct Sequence Spread Spectrum)* – means spectrum dispersion using direct sequence, DS acronym is also used in literature. DSSS divides the band into separate channels. A device never transmits for too long using one frequency within one channel. A lot of different networks may overlap if they use different channels within the same range and it does not cause any interferences (Engst and Fleishman 2005). In order to spread a radio signal in one channel which is 22 MHz wide without the necessity of changing the frequency, DSSS technology uses a spread method called “chipping code” (11- Chip Barker). Each connection in the DSSS system uses one channel, and it is not necessary to change the frequency. Transmission in the DSSS system uses a broader bandwidth. However, it requires smaller power than a conventional signal.

**Table 3.1.** Channels allocation for wireless networks of Ethernet type

| Channel number | Frequency MHz (countries) |
|---|---|
| 1 | 2412 (USA, Europe, Japan ) |
| 2 | 2417 (USA, Europe, Japan) |
| 3 | 2422 (USA, Europe, Japan) |
| 4 | 2427 (USA, Europe, Japan) |
| 5 | 2432 (USA, Europe, Japan) |
| 6 | 2437 (USA, Europe, Japan) |
| 7 | 2442 (USA, Europe, Japan) |
| 8 | 2447 (USA, Europe, Japan) |
| 9 | 2452 (USA, Europe, Japan) |
| 10 | 2457 (USA, Europe, France, Japan) |
| 11 | 2462 (USA, Europe, France, Japan) |
| 12 | 2467 (Europe, France, Japan) |
| 13 | 2472 (Europe, France, Japan) |
| 14 | 2484 (only Japan) |

Source: Ross (2005)

The values of the frequencies around 2.4 GHz that are made available differ slightly in different parts of the world. However, frequency ranges overlap to a great degree, which allows for using the same equipment all over the world (though it may sometimes be necessary to change the number of channel set on the network card into another), Table 3.1 (Ross 2005).

# 4 Wi-Fi standards

*802.11b* – this standard was introduced in October 1999. It provides transmission and receipt of data with the speed of 11 Mb/s. However, the actual capacity for the end-user equals 4 to 5 Mb/s. This is caused by significant load of the capacity generated by packets' headers, transmission and other elements. Access to the carried is obtained using CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) method. In case a few devices are trying to send data over the same connection at the same time, a collision of transmitted packets occurs, which results in the loss of transmitted data. CSMA/CA provides the method of fair access to the carrier and decides who and when can send data.

CSMA/CA operates in the following way. Before data transmission, a device that intends to send them, listens to the state of the connection and checks if there is no other transmission in progress. A transmission may only begin if no signal has been detected which may indicate that another device has started transmission. The device which is not sending data listens all the time whether the data aren't addressed to it. If two devices which want to send information did not detect traffic in the network and started their transmissions simultaneously, then a collision occurs and the data are lost. At the moment of sending data, a device monitors its own transmission, and if it detects a collision, it stops sending data and sends a signal informing about the collision (jam signal). Transmission may be resumed after a randomly selected period of time and checking whether the transmission channel is idle.

*802.11g* – this standard was introduced in June 2003. It uses, just like specification 802.11b, the frequency of 2.4 GHz. New techniques that were used, allowed its authors to reach the transfer of 54Mb/s. Transmission technique which allows for such high capacity of the network is called OFDM (Orthogonal Frequency-Division Multiplexing), where a single data stream is coded in many subcarriers. In the OFDM transmission system 52 subcarriers are used, for which such modulations as BPSK, QPSK or QAM/64-QAM (Quadrature Amplitude Modulation) are used. The maximum transmission speed (54 Mbit/s) is obtained for 64-QAM modulation (216 bits of data for one OFDM symbol) (http://pl.wikipedia.org). At present, 802.11g may strengthen its position on the market, due to its compatibility with only one preceding standard.

*802.11n* – this standard was omitted as it is a new technology, which is still being developed. During this paper compilation, there is only a draft for the future standard, anticipated time of the introduction of this standard was 2008 and it was postponed to mid-2010.

## 5 Wireless networks topologies

There are two types of wireless networks topologies, called work modes, namely: ad hoc (Lat. to this) and infrastructure.

*Ad hoc* – this is the simplest method of interconnecting devices using wireless connectivity. Each device may be an end terminal as well as a router. Lack of access points does not require any infrastructure for data transmission, Figure 5.1.

In order to limit access to the network, a domain identifier (Wireless Domain ID) is used, which is placed on the computer that is a part of a network and provides connectivity with other members of the group. The distance between individual workstations ranges between 30 and 60 metres. The solution is optimum for small companies, shop floors and conference rooms.

*Infrastructure* – the topology is dedicated for more complex structural networks that have at least one device supervising proper functioning of the network – access point. An access point (AP) is a bridge connecting a wireless and a wire network; it may be a device dedicated to this task as well as an ordinary computer with appropriate software and peripherals. Moreover, it ensures synchronization, coordination, packet broadcast and transmission. A standard that allows a network with one AP to function is called BSS (Basic Service Set).

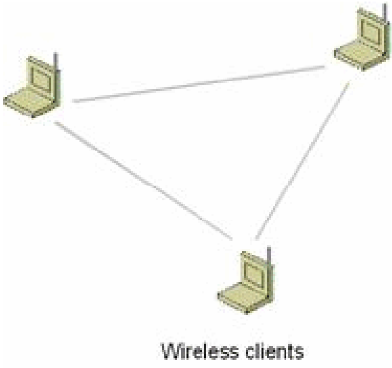

**Figure 5.1.** Ad hoc topology
Source: http://www.hotspot.info.pl/pictures/articles/WiFiSO02.gif

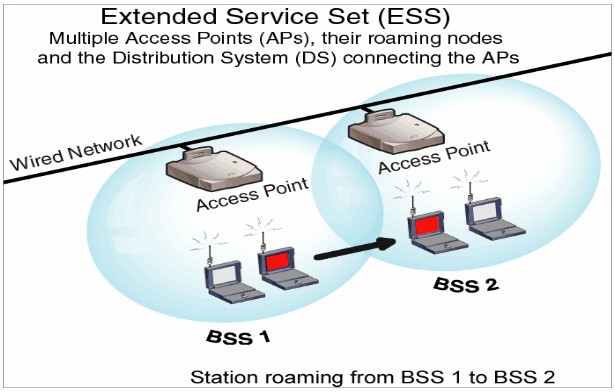
Extended Service Set (ESS)
Multiple Access Points (APs), their roaming nodes and the Distribution System (DS) connecting the APs
Wired Network
Access Point
Access Point
BSS 1
BSS 2
Station roaming from BSS 1 to BSS 2

**Figure 5.2.** ESS infrastructure topology
Source: http://www.wildpackets.com/images/compendium/topo-2b_2.gif

In networks that cover large areas using one AP may not be enough. Using two or more access points is called ESS ( Extender Service Set); it is a connection of at least two BSSs connected to the same cable network, Figure 5.2. When the BSSs operation ranges overlap even to a small degree, there occurs so called roaming between individual BSSs. A device that is changing position may change the access point it is using provided that it offers better conditions (provides stronger signal).

In ESS networks a major problem occurs when our network overlaps with another network. The devices that want to work in one network have to use the same SSID (Service Set IDentifier) number. Network identifier SSID is not encrypted during transmission and is available. Hence, using it as a protection against potential unauthorized attempts of getting access to the network is not recommended (Roshan and Leary 2005, Roshan and Leary 2006; http://www.wildpackets.com, Santi 2005, Gast 2005).

# 6 Design assumptions

*Company characterization* – a new company is set up and it is located on one floor of a building. There is going to be 21 workstations, each with one PC; moreover, at least 6 employees use laptops. Wireless LAN network with access to the Internet must provide contact with other companies. Moreover, the network must guarantee efficient use of local hardware such as printers.

*Plans and description of rooms* – The room is adapted for teleinformatics cabling installation. There is going to be a room for IT specialists, where hardware that allows a computerized company to function is to be located. An ISP (Internet Service Provider) company provides access to the Internet, and it guarantees connections to the network via xDSL (xDigital Subscriber Line) technology.

*Hardware* – hardware compatible with standard 802.11g may be used for LAN network construction. WRT54GL – will be an access point as it has a built-in broadband router (for xDSL services) and it has 4-port FastEthernet switch. The device provides roaming, balancing the load and packet traffic filtering. It supports the following technologies: WPA (*Wi-Fi Protected Access*), 128-bit encryption WEP (*Wireless Equivalent Privacy*), SES (Secure Easy Setup). There is also a possibility to define access or access denial depending on clients' cards' MAC addresses or IP numbers. As a router, it also has a build-in firewall. The range of the device in the open space is equal to about 100 metres. Despite architectural obstacles in the form of walls dividing individual rooms, one device is able to cover the area of the whole office. However, for the reason of providing redundancy in the network and potential expansion of network infrastructure using two access points seems justified. Another device in a LAN network is wireless network card WMP54G for PCI, which may work in *ad-hoc* mode (sole network cards) as well as *infrastructure* (as a client of an access point), has SES function, supports WEP (128-bit) and WPA encryption. Laptops will be equipped in wireless network card WPC54G for PCMCIA type 2. It supports WEP 40 and 128-bit as well as WPA, has SES function. One-section locked rack cabinet, type NWE-4A06/GL/ZS with a metal door and a glass front – for a modem.

# 7 Wi-Fi network security

In order to secure the network, protocol WPA/AES (WPA2), which requires RADIUS server, will be used. At present, this solution is considered the safest one. Moreover, there will be a built-in firewall on the router, and it will be a first obstacle for potential attempts of violating network's security. Apart from protection against outside attacks, it is possible to block its selected ports or ports ranges, which, given proper configuration, will increase employees' efficiency and productivity by blocking access to internet communicators (gadu gadu, tlen, etc.). An additional advantage of the router is a DMZ zone – demilitarized zone; it is a zone of internal network. This zone usually has servers providing services to external clients, and, as such, the servers are more exposed to attacks. However, putting servers in DMZ makes it possible to block access to the internal company network in case of hacking.

Each computer, apart from a firewall, should be equipped in its own local protection software.

The issue of Wi-Fi networks security is a key issue during the implementation phase both in companies as well as private households. In case of introduction of new stricter safety policies and regulations in companies, static connections between MAC and IP may be used, which will grant the company employees exclusive access to the company network.

# 8 Implementation and project estimate

Access points shall be mounted on the ceiling in order to make the signal stronger. Local network is to connect with the global network using ISP services and connecting first access point (AP1) using WAN port with the device supplied by the ISP. Due to security reasons, access to modem should be restricted. Therefore, the modem will be placed in a locked rack cabinet. The other (redundant) access point (AP2) will be connected with the network using a copper wire UTP 5. In this configuration AP1 device will also be and external gate. Measuring the cable length, the length of 2.5 metres (from the rack cabinet to the suspended ceiling) should be taken into account. Moreover, 10% of the estimated total length should be added (it is better to have some spare wire than make a new cabling) due to practical reasons. In desktop computers a WMP54G network card with the RJ45 will be used instead of a standard one. At present, most notebooks is equipped in an internal wireless network card. However, it there will be a few-year-old models without such a card, there is a possibility to purchase a PCMCIA compatible WPC54G network card.

<u>Cost estimate</u>

The total length of UTP cable cat. 5 ≈ 17 m (15.7 m + 10%) – 20.5 PLN, 2 WRT54GL devices - 488 PLN, 21 WMP54G cards - 2835 PLN, 6 WPC54G cards - 762 PLN (in case laptops do not have them), 4 RJ45 plugs - 2 PLN, 1 rack cabinet-465 PLN. All the prices are gross prices.

The total cost of equipment purchase together with the cabling is equal to 4572.5 PLN (or 3810.50 PLN. If the laptops are equipped in Wi-Fi cards compatible with IEEE 802.11g).

# 9 Summary

**Table 9.1.** Differences between wireless and cable networks

| | P1 | P2 |
|---|---|---|
| Easy assembly | + | - |
| Mobility | + | - |
| Easy addition of a new computer to a network | + | - |
| Susceptibility to transmission interference | - | + |
| Maximum obtainable capacity | 3.3(3) Mb/s* | 100 Mb/s |
| Possibility of transmission monitoring | - | + |

P1- wireless network, P2- a network based on copper cable, „+” - favourable, „-” – unfavourable (* - using 21 workstations simultaneously)

A wireless network is a mobile technology; in case of moving location, it is enough to move access points and the network is ready for use. Networks based on cables (copper wires, fibre optic cable), except for the cables connecting computers with wall sockets, may be used only in a particular place. It is not possible to move them to a new location. Table 9.1 shows advantages and disadvantages of wireless and cable networks.

# 10 Conclusions

1. At present, a new, rapidly developing Wi-Fi technology has ceased to be available to rich companies only.
2. The main and the only drawback of radio networks is the issue of protecting them against hacking attempts. However, proper and professional configuration of hardware can eliminate this problem to a great extent.
3. Standard 802.11g by its mobility, range, easy installation and assembly may be used without major problems in companies that belong to SMB sector.

Continuous work on development of technology 802.11, will result in growing number of supporters and users. A presentation of a new standard that belongs to 802.11 family marked with the symbol n is announced for mid-2010, and it will undoubtedly cause a decrease in the number of companies using copper cabling. Justifiability and cost-effectiveness of Wi-Fi is obvious. However, it is necessary to remember that there will always be a small group of companies whose specification will impose older solutions. Moreover, companies that have been on the market for a long time already have network infrastructures, and this contributes to the fact that copper cabling will not disappear suddenly. However, new companies, having acquainted themselves with the possibilities Wi-Fi provides, should choose a new, mobile technology.

## References

1. Rozporządzenie Komisji Wspólnot Europejskich (WE) nr 364/2004 z dnia 25 lutego 2004 r. zmieniające rozporządzenie (WE) nr 70/2001 i rozszerzające jego zakres w celu włączenia pomocy dla badań i rozwoju. Dostępny w Internecie: http://209.85.135.104/search?q=cache:TSniWN1EDF0J.
2. Kwartalnik SAP Polska Nr 2(18)/2004 Strategie biznesu. Dostępny w Internecie: http://www.sap.com/poland/company/strategie/18/temat_numeru/strategia_sap/index.epx.
3. Zieliński B. 2000. Bezprzewodowe sieci komputerowe. Wydawnictwo Helion. ISBN: 83-7197-324-1.
4. Wrocławski R. 2000. Transmisja danych z komórki. Dostępny w Internecie: http://www.fkn.pl/ 2,3699,1357713,1,1,artykul.html.
5. http://pl.wikipedia.org/wiki/IrDA, http://en.wikipedia.org/wiki/Irda.
6. http://pl.wikipedia.org/, http://www.bluetooth.com.
7. http://www.pc.co.il/.
8. http://pl.wikipedia.org.
9. http://en.wikipedia.org.
10. http://www.hotspot.info.pl/pictures/articles/WiFiSO02.gif.
11. http://www.wildpackets.com/images/compendium/topo-2b_2.gif.
12. Engst A., Fleishman G. 2005. Sieci bezprzewodowe praktyczny przewodnik. Tytuł oryginalny: The Wireless 13. Networking Starter Kit. Secondo Editio. Tłumaczenie Jarczyk A. Wydawnictwo Helion. ISBN: 83-7361-977-1.
14. Ross J. 2005. Sieci standardu Wi-Fi. Wydawnictwo Nakom. ISBN: 83-89529-03-3.
15. Roshan P., Leary J. 2005. Akademia sieci CISCO CCNA semestr 1 i 2. Wydanie trzecie, poprawione. Wydawnictwo Mikom, Warszawa. Tytuł oryginalny: Cisco Networking Academy Program CCNA 1 and 2 Companion Guide. Third Editio, by Cisco Systems, Inc. ISBN: 83-7279-495-2.
16. Roshan P., Leary J. 2006. Bezprzewodowe sieci LAN 802.11. Wydawnictwo Mikom, Warszawa. SBN: 83-01-14858-6.
17. Santi P. 2005. Topology Control in Wireless Ad Hoc Sensor Networks. Wydawnictwo John Wiley & Sons, Ltd. ISBN-13 978-0-470-09453-2.
18. Gast M. 2005. 802.11 Wireless Networks: The Definitive Guide, Second Edition. Wydawnictwo O’Reilly. ISBN 10:0-596-10052-3.