Dariusz CHAŁADYNIAK[1]

WYBRANE TECHNOLOGIE BEZPRZEWODOWEJ TRANSMISJI DANYCH

Streszczenie

Artykuł dotyczy podstawowych informacji o możliwościach i działaniu wybranych technologii bezprzewodowych (IrDA, Bluetooth, Wi-Fi, WiMAX). Omówione zostały ich podstawowe parametry, standardy oraz zastosowanie. W artykule pojawią się również zagadnienia dotyczące bezpieczeństwa sieci bezprzewodowych. Dodatkowo zostaną przybliżone zjawiska warchalking'u i wardriving'u.

Abstract

The paper concerns basic information about capabilities and performance of selected wireless Technologies (IrDA, Bluetooth, Wi-Fi, WiMAX). Their basic parameters, standards and applications were discussed. The paper will also include issues concerning wireless networks safety. Additionally, warchalking and wardriving will be explained.

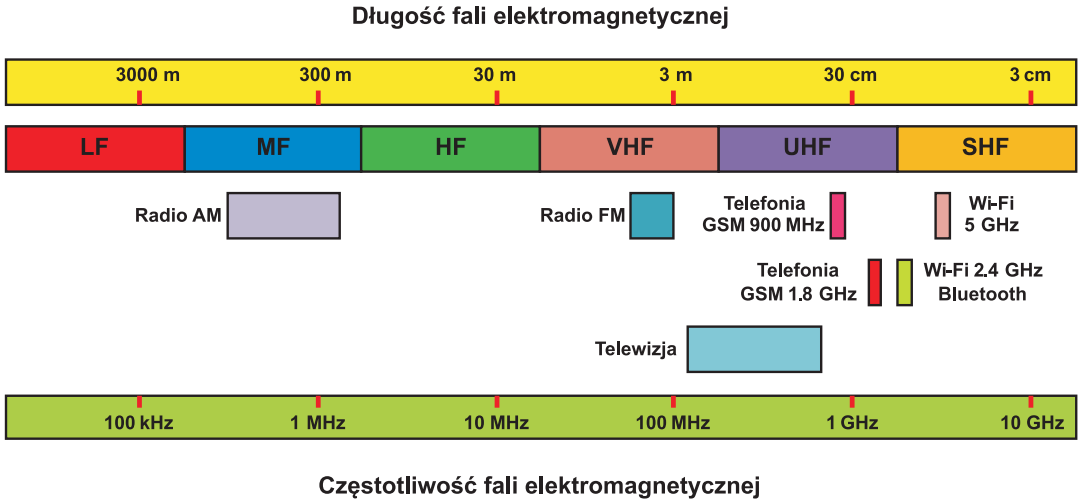
1. WSTĘP DO SIECI BEZPRZEWODOWYCH

Sieci bezprzewodowe (ang. *wireless networks*) są bardzo ciekawą alternatywą dla klasycznych sieci przewodowych. Wszędzie tam, gdzie te drugie są mało ekonomicznym rozwiązaniem stosuje się sieci WLAN. Sieci bezprzewodowe jako medium transmisyjne wykorzystują fale radiowe (elektromagnetyczne) albo fale podczerwone.

1.1 Spektrum fal elektromagnetycznych

Spektrum fal elektromagnetycznych (rys. 1.1), często występujące również pod pojęciem widma fal, jest przedstawieniem fal w zależności od ich częstotliwość lub długości. Widmo fal elektromagnetycznych obejmuje takie fale, jak fale radiowe,

[1] Dr inż. Dariusz Chaładyniak jest wykładowcą Warszawskiej Wyższej Szkoły Informatyki.



Rys. 1.1. Spektrum fal elektromagnetycznych

mikrofale, promieniowanie widzialne, promieniowanie podczerwone, ultrafioletowe, promieniowanie gamma, czy promieniowanie rentgenowskie.

W sieciach bezprzewodowych Wi-Fi i Bluetooth wykorzystuje się fale radiowe a w sieciach IrDA – fale w kanale podczerwieni. Na rys. 1 można zaobserwować, że dłuższym falom odpowiadają mniejsze częstotliwości i odwrotnie, krótszym falom odpowiadają wyższe częstotliwości. Częstotliwość fali wyrażana jest w hercach (Hz) i określa ilość cykli fali w ciągu sekundy.

1.2 Metody modulacji

Przesyłanie mowy, muzyki i innych dźwięków za pomocą fal radiowych polega na zmianie (czyli modulacji) sygnału prądu przemiennego tzw. nośnej sygnału. Każdy rodzaj bezprzewodowej sieci transmisji danych działa w określonym paśmie częstotliwości radiowych (2.4 GHz, 5 GHz).

W sieciach bezprzewodowych wykorzystuje się trzy rodzaje modulacji:

1. DSSS (ang. *Direct Sequence Spread Spectrum*) – technologia rozszerzonego widma z bezpośrednim szeregowaniem bitów. Strumienie danych są tu rozdzielane przy transmitowaniu z wykorzystaniem specjalnych bitów (zwanych bitami szumów), a odbiornik musi dysponować układem deszyfrującym (który wykorzystuje tzw. *chipping code*, interpretując w odpowiedni sposób poszczególne strumienie danych). Cały proces polega na rozbiciu informacji na wiele „podbitów", dzięki czemu pakiety są transmitowane przy użyciu dużo szerszego pasma przenoszenia danych niż w przypadku normalnej transmisji.

2. FHSS (ang. *Frequency Hopping Spread Spectrum*) – strumienie danych są przełączane z jednej częstotliwości na drugą (a każda częstotliwość to oddzielny kanał komunikacyjny), pozostając na każdej z nich nie dłużej niż 100 ms.
3. OFDM (ang. *Orthogonal Frequency Division Multiplexing*) – została tak zoptymalizowana, aby interfejs bezprzewodowy mógł transmitować dane w środowiskach pełnych zakłóceń, takich jak zatłoczone obszary miejskie.

1.3 Standardy sieci bezprzewodowych

Sieci bezprzewodowe opierają się przede wszystkim na standardach z rodziny IEEE 802. IEEE. W tej rodzinie sieci bezprzewodowych dotyczy grupa standardów IEEE 802.11. Rodzina 802.11 obejmuje trzy zupełnie niezależne protokoły skupiające się na kodowaniu (a, b, g). Pierwszym powszechnie zaakceptowanym standardem był 802.11b, potem weszły 802.11a oraz 802.11g. Standard 802.11n nie jest jeszcze oficjalnie zatwierdzony, ale coraz więcej sprzętu sieciowego jest kompatybilna z tą technologią.

Tabela 1.1. Standardy sieci bezprzewodowych

Nazwa standardu	Częstotliwość radiowa	Zasięg sygnału	Maksymalna szybkość transmisji
802.11 b	2.4 GHz	30 metrów	11 Mb/s
802.11a	5 GHz	30 metrów	54 Mb/s
802.11 g	2.4 GHz	30 metrów	54 Mb/s
802.11 n	2.4 GHz / 5 GHz	50 metrów	600 Mb/s
802.15.1 Bluetooth	2.4 GHz	10 metrów	2 Mb/s

Pierwszym standardem sieci radiowej był opublikowany w 1997 roku IEEE standard 802.11. Umożliwiał on transmisję z przepustowością 1 oraz 2 Mb/s przy użyciu podczerwieni bądź też pasma radiowego 2.4 GHz. Urządzenia tego typu są już praktycznie nie stosowane.

Standard 802.11b został zatwierdzony w 1999 roku. Pracuje w paśmie o częstotliwości 2.4 GHz. Umożliwia maksymalną teoretyczną szybkość transmisji danych do 11 Mb/s. Zasięg jego działania jest ograniczony do 30 metrów w pomieszczeniu i do 100 m w przestrzeni otwartej.

Standard 802.11a został zatwierdzony w 1999 roku. Pracuje w paśmie częstotliwości 5 GHz. Jego maksymalna teoretyczna przepływność sięga 54 Mb/s.

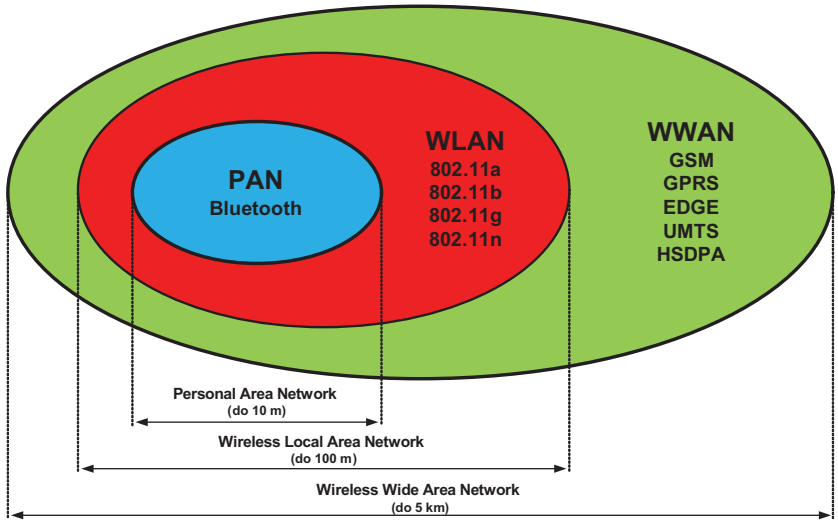
Standard 802.11g oficjalnie został zatwierdzony w 2003 roku. Pracuje podobnie jak standard 802.11g w paśmie o częstotliwości 2.4 GHz. Umożliwia osiągnięcie maksymalnej teoretycznej szybkości transmisji danych do 54 Mb/s. Zasięg jego działania w budynku ograniczony jest do 30 metrów natomiast w przestrzeni otwartej dochodzi do 100 metrów.

Najnowszy standard 802.11n (zatwierdzony w 2009 roku) może działać w paśmie radiowym o częstotliwości 2.4 GHz lub 5 GHz. Zapewnia maksymalną przepływność przesyłu danych do 600 Mb/s. Zasięg jego działania został wydłużony do 50 metrów w pomieszczeniach.

1.4 Podział zasięgu sieci bezprzewodowych

Pod względem zasięgu działania (patrz rys. 1.2) sieci bezprzewodowe możemy podzielić na trzy kategorie:

1. Sieci PAN (ang. *Personal Area Network*) – działają na odległości do 10 metrów. Jako przykład tej sieci można podać standard Bluetooth.
2. Sieci WLAN (ang. *Wireless Local Area Network*) – działają w zakresie do 100 metrów w otwartej przestrzeni. Przykłady tych sieci to standardy IEEE 802.11a/b/g/n.
3. Sieci WWAN (ang. *Wireless Wide Area Network*) – działają na odległości nawet do 5 kilometrów. To przede wszystkim systemy sieci telefonii komórkowej (GSM, GPRS, EDGE, UMTS, HSDPA).



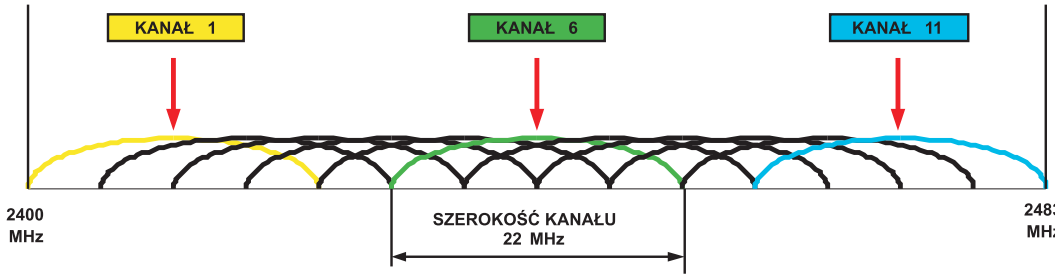
Rys. 1.2. Podział zasięgu sieci bezprzewodowych

2. TECHNOLOGIA WI-FI

Technologia Wi-Fi polega na bezprzewodowej łączności w dwóch zakresach częstotliwości: 2.4 GHz oraz 5 GHz.

Rys. 2.1. Przykłady urządzeń wykorzystujących technologię Wi-Fi

2.1 Kanały transmisyjne

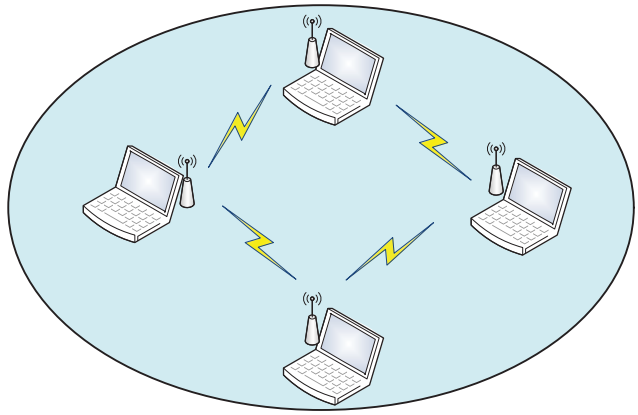


Rys. 2.2. Kanały transmisyjne

Dokładna częstotliwość stosowana w określonej sieci bezprzewodowej zależy od wykorzystywanego kanału transmisyjnego. Na przykład w USA używa się 11 kanałów, w Polsce 13, w Japonii 14 a we Francji tylko 4. Aby zachować światowy standard, na całym świecie używa się tej samej numeracji kanałów czyli kanał nr 6 w Warszawie odpowiada tej samej częstotliwości co w Tokio czy Los Angeles. W przypadku wyjazdu za granicę może być konieczne przestawienie karty sieciowej na inny kanał, aczkolwiek robią one to automatycznie. Jeśli nie mamy pewności, z jakich kanałów można korzystać w danym kraju, wystarczy sprawdzić to w lokalnym urzędzie regulacyjnym. Niezależnie od tego można skorzystać z kanałów o numerach 10 i 11, które są dostępne na całym świecie (poza Izraelem).

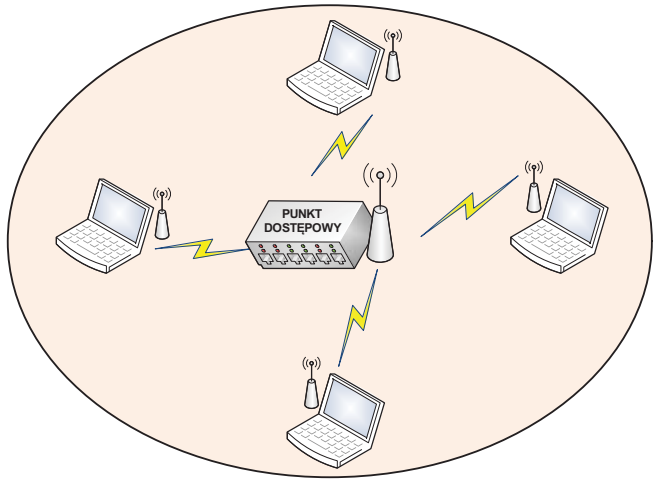
2.2 Technologia sieci ad-hoc – IBSS

Sieci Wi-Fi mogą działać w dwóch trybach pracy: *ad hoc* (równorzędnym) i infrastrukturalnym. Sieć w technologii *ad-hoc*, określana mianem IBSS (ang. *Independent Basic Service Set*) może być wykorzystana do wymiany danych między kilkoma komputerami bez użycia punktu dostępowego, ale i bez dostępu do istniejącej struktury sieciowej.



Rys. 2.3. Technologia sieci ad-hoc

2.3 Technologia sieci infrastrukturalnej – BSS

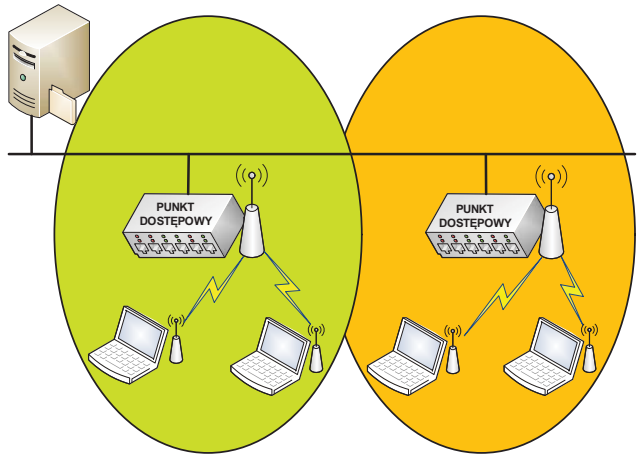


Rys. 2.4. Technologia sieci infrastrukturalnej BSS

W skład sieci infrastrukturalnej wchodzi zwykle jeden lub więcej punktów dostępowych, które przyłączone są przeważnie do istniejącej przewodowej lokalnej sieci komputerowej. Każda stacja bezprzewodowa wymienia komunikaty i dane z punktem dostępowym, które są przekazywane dalej do innych węzłów sieci LAN lub WLAN.

Sieć infrastrukturalna, zawierająca tylko jedną stację bazową (punkt dostępowy, router), jest określana mianem BSS (ang. *Basic Service Set*).

2.4 Technologia sieci infrastrukturalnej – ESS



Rys. 2.5. Technologia sieci infrastrukturalnej ESS

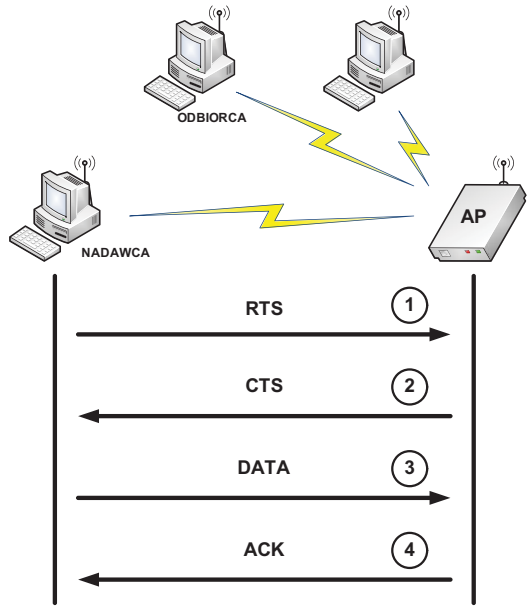
Jeśli infrastrukturalna sieć bezprzewodowa korzysta z kilku punktów dostępowych, określa się ją mianem ESS (ang. *Extended Service Set*).

2.5 Metoda dostępu CSMA/CA

Metoda dostępu CSMA/CA (ang. *Carrier Sense with Multiple Access/Collision Avoidance*), stosowana w sieciach bezprzewodowych, polega na unikaniu kolizji.

W sieciach WLAN nie jest możliwe stosowanie używanego w sieciach LAN mechanizmu CSMA/CD (ang. *CSMA/Collision Detection*). Stacja próbująca nadawać nie może bowiem jednocześnie nasłuchiwać kanału, gdyż jej własny sygnał zagłuszałby wszystkie inne. Stacja chcąca nadawać prowadzi nasłuch pasma: jeśli przez określony czas nie wykryje transmisji, przełącza się w tryb gotowości do nadawania i czeka określony czas. Następnie, jeśli nadal nikt nie prowadzi nadawania, stacja rozpoczyna transmisję. Mechanizm ten jest określany skrótem CCA (ang. *Clear*

Channel Assessment). Dodatkowo, dla każdej przesłanej ramki, do nadawcy musi dotrzeć potwierdzenie poprawności otrzymania danych, wysłane przez odbiorcę ACK (ang. *Acknowledge*).



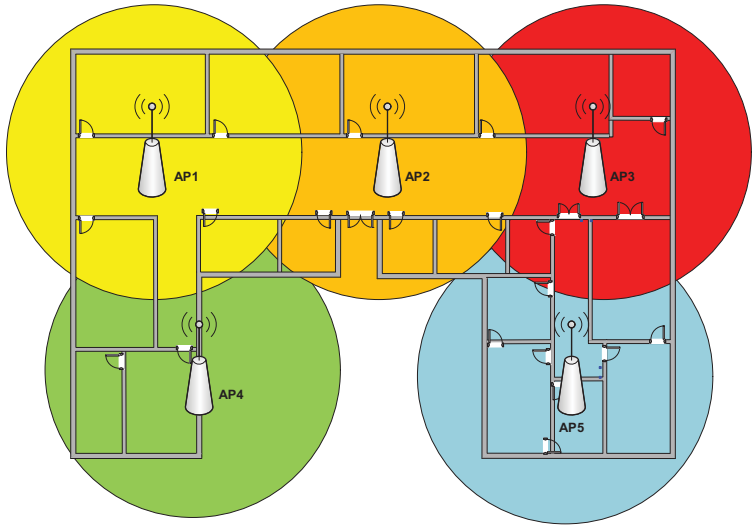
Rys. 2.6. Schemat działania metody CSMA/CA

Ponieważ stacje mogą być oddalone od siebie na odległość większą od swojego zasięgu nadawania, mechanizm CCA nie spełnia swoich zadań. W tym przypadku stacja nadawcza najpierw wysyła ramkę RTS (1) (ang. *Request To Send*), będącą informacją dla pozostałych stacji w jego zasięgu o zamiarze nadawania. Następnie Punkt dostępowy (AP) wysyła ramkę CTS (2) (ang. *Clear To Send*), informującą o gotowości do odbioru. Sygnał CTS dotrze do wszystkich stacji w zasięgu (wiadomość typu rozgłoszenie), czyli dotrze również do stacji odbiorczej, która dzięki temu zostanie powiadomiona o rozpoczynającej się transmisji. Po wymianie ramek RTS i CTS rozpoczyna się właściwa transmisja ramki (3) (DATA), której otrzymanie odbiorca potwierdza ramką ACK (4). Jeśli nadawca nie dostanie potwierdzenia ACK, musi ponowić transmisję danych.

2.6 Rozmieszczenie punktów dostępu

Jeden punkt dostępu (AP) może być całkowicie wystarczający do obsługi bezprzewodowej sieci lokalnej w domku jednorodzinnym lub w małej firmie. Jeśli jednak sieć ma obejmować większy obszar (o średnicy ponad 30 metrów), to są potrzebne

dodatkowe punkty dostępu. Specyfikacja Wi-Fi zawiera funkcję *roamingu*, która automatycznie przestawia połączenie sieciowe z jednego punku dostępu do innego, gdy jakość sygnału udostępnianego przez nowy punkt jest lepsza niż jakość sygnału obsługującego oryginalne połączenie.



Rys. 2.7. Przykładowe rozmieszczenie punktów dostępu

Punkty dostępu powinny być tak rozmieszczone, aby ich obszary oddziaływania zachodziły na siebie ale jednocześnie działały na kanałach o innych numerach. Aby maksymalnie zmniejszyć zakłócenia pomiędzy nimi, każda para sąsiadujących ze sobą punktów dostępu powinna mieć przydzielone kanały odległe o co najmniej pięć numerów.

W większości przypadków, jeśli korzysta się z wielu punktów dostępu, powinny być one rozmieszczone w taki sposób, aby obszary oddziaływania sąsiednich punktów nakładały się na siebie w około 30 procentach (patrz rys. 2.7).

2.7 Bezpieczeństwo sieci Wi-Fi

Sieci bezprzewodowe są bardzo narażone na zagrożenia sieciowe. Narzędzia bezpieczeństwa w specyfikacji Wi-Fi nie są doskonałe, ale mogą w miarę skutecznie je zabezpieczyć. Poniżej przedstawiamy najważniejsze mechanizmy bezpieczeństwa w sieciach bezprzewodowych:

1. Identyfikator SSID (ang. *Service Set ID*) – wszystkie punkty dostępu oraz wszyscy klienci znajdujący się w sieci muszą mieć ustawiony taki sam SSID. Identyfikator ten zapewnia pewną bardzo ograniczoną formę kontroli dostępu,

ponieważ trzeba go podać w trakcie nawiązywania połączenia do sieci Wi-Fi i jest on wartością tekstową, którą można dowolnie określić. Większość punktów dostępu rozsyła zwykle sygnał kontrolny, który rozgłasza identyfikator SSID danej sieci. Gdy karta sieciowa przeprowadza skanowanie sygnałów radiowych, wykrywa je i wyświetla listę znalezionych identyfikatorów SSID w swoim programie kontrolnym (można również tę funkcję wyłączyć).

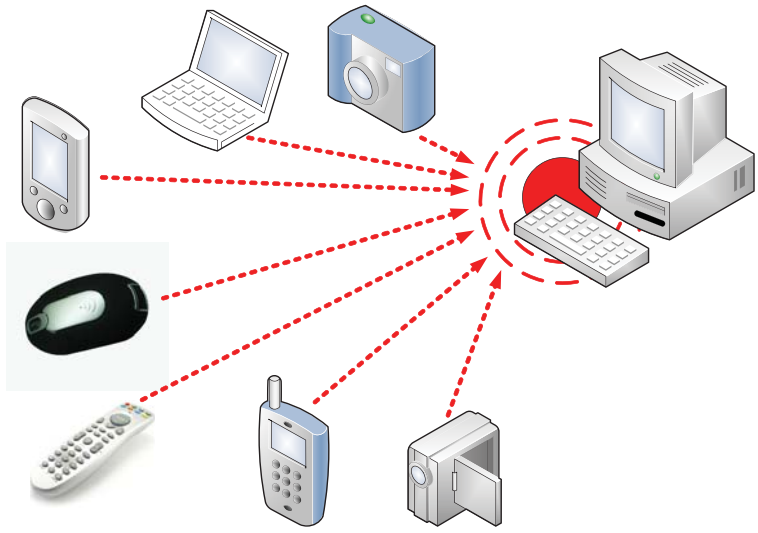
2. Szyfrowanie WEP (ang. *Wired Equivalent Privacy*) – jest dostępne w każdym systemie działającym w standardzie Wi-Fi. Szyfrowanie to bazuje na współdzielonym kluczu szyfrującym o długości 40 lub 104 bitów oraz 24-bitowym wektorze inicjującym.
3. Standard 802.1x – scentralizowanie identyfikacji użytkowników, uwierzytelnianie, dynamiczne zarządzanie kluczami. Wszystkie te środki zapewniają dużo większe bezpieczeństwo w sieci niż kontrola dostępu wbudowana w protokół 802.11.
4. Szyfrowanie WPA (ang. *Wi-Fi Protected Access*) – znacznie bezpieczniejsze szyfrowanie niż WEP, ponieważ używa protokołu TKIP (ang. *Temporal Key Integrity Protocol*) w celu automatycznej zmiany klucza szyfrującego po upływie określonego czasu lub gdy nastąpi wymiana określonej liczby pakietów. Na szyfrowanie WPA składają się poniższe składniki:
   – WPA = 802.1x + EAP + TKIP + MIC
   – EAP (ang. *Extensible Authentication Protocol*)
   – TKIP (ang. *Temporal Key Integrity Protocol*)
   – MIC (ang. *Message Integrity Check*)

3. TECHNOLOGIA IRDA

W technologii IrDA (ang. *Infrared Data Association*) jest wykorzystywana silnie skupiona wiązka światła w paśmie podczerwieni (850-900 nm). Koniecznym warunkiem zastosowania tej technologii jest bezpośrednia widoczność nadajnika i odbiornika.

Podstawowe właściwości technologii IrDA to:

1. Prosta i tania implementacja;
2. Mały pobór mocy;
3. Połączenie typu punkt-punkt;
4. Długość fali świetlnej: 850 – 900 nm;
5. Zasięg: do 10 metrów;
6. Kąt wiązki transmisji: 30°.



Rys. 3.1. Przykłady urządzeń wykorzystujących technologię IrDA

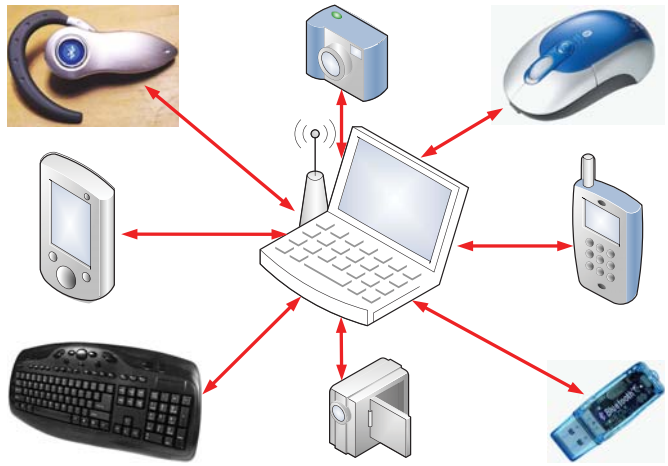
Tabela 3.1. Wybrane parametry technologii IrDA

Tryb transmisji	Szybkość transmisji
Serial InfraRed SIR	2.4 - 115.2 kbps
Medium InfraRed MIR	0.576 - 1.15 Mbps
Fast InfraRed FIR	1.15 - 4 Mbps
Very Fast InfraRed VFIR	16 Mbps

4. TECHNOLOGIA BLUETOOTH

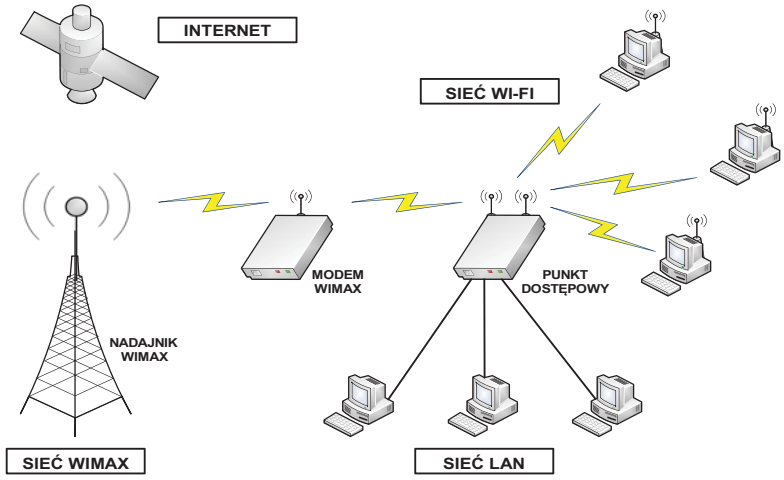
Technologia Bluetooth (patrz rys. 4.1) jest globalną inicjatywą bezprzewodowego dostępu radiowego grupy producentów: Ericsson, IBM, Intel, Nokia i Toshiba. Standard Bluetooth powstał w 1994 roku w Szwecji. Jego nazwa pochodzi od przydomka żyjącego w X wieku duńskiego króla Haralda I – *Blaatand* (czyli Sinozęby).

Technologia Bluetooth jest standardem połączeń radiowych o ograniczonym zasięgu, między telefonami komórkowymi, komputerami przenośnymi, urządzeniami peryferyjnymi (klawiatury, myszy, monitory, drukarkami), a także audiowizualnymi (piloty, odbiorniki TV i radiowe). W Bluetooth stosuje się bezkierunkowe łącze radiowe o niewielkim zasięgu (do 10 m), o częstotliwościach pracy w paśmie 2,402-2,480 GHz. Możliwa jest komunikacja między różnymi urządzeniami przenośnymi (maks. 256) z przepływnością do 1 Mb/s.



Rys. 4.1. Przykłady urządzeń wykorzystujących technologię Bluetooth

5. TECHNOLOGIA WIMAX



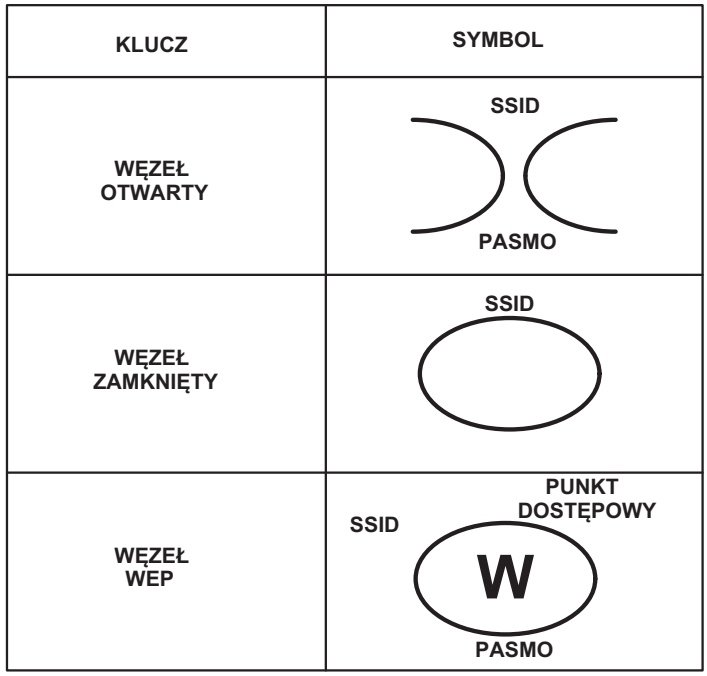
Rys. 5.1. Schemat działania technologii WiMAX

Technologia WiMAX (ang. *Worldwide Interoperability for Microwave Access*) – to bezprzewodowa metoda szerokopasmowej transmisji danych na dużych obszarach geograficznych. Jest to bezprzewodowa sieć miejska, w której zazwyczaj stosuje się jedną lub więcej stacji bazowych, z których każda dystrybuuje sygnał drogą radiową w promieniu do 50 km. Oficjalnie technologia WiMAX jest opisana w specyfikacji

IEEE 802.16d. Każdy dostawca usługi WiMAX korzysta z koncesjonowanych częstotliwości z zakresu pomiędzy 2 GHz a 11 GHz. Łącze WiMAX może teoretycznie przesyłać dane z przepływnością do 70 Mb/s.

6. WARCHALKING, WARDRIVING

6.1 Warchalking



Rys. 6.1. Oryginalne znaki naznaczonego dostępu

Anglik Matt Jones zaczął w czerwcu 2002 roku rysować w Londynie kredą na chodnikach i ścianach domów symbole identyfikujące miejsca, do których dochodzą sygnały sieci bezprzewodowych IEEE 802.11b i jest możliwe uzyskanie „bezpłatnego" dostępu do Internetu. Na rysunku 6.1 przedstawiono trzy oryginalne znaki naznaczonego dostępu

Na powyższym rysunku przedstawiono propozycję nowych znaków naznaczonego dostępu do sieci Internet. Znaki te są malowane za pomocą kredy, by osoba oznaczająca punkt dostępu nie została posądzona o wandalizm, jak to bywa w przypadku graffiti wykonanego sprayem (kredę łatwo można zmyć).

KLUCZ	SYMBOL
NIEOGRANICZONY DOSTĘP	
DOSTĘP OTWARTY Z OGRANICZENIAMI	
PUNKT DOSTĘPOWY Z WEP	W
PUNKT DOSTĘPOWY Z ZAMKNIĘTYM ESSID	

KLUCZ	SYMBOL
PUNKT DOSTĘPOWY Z FILTROWANIEM ADRESÓW MAC	
PŁAĆ ZA DOSTĘP DO PUNKTU DOSTĘPOWEGO	$
PUNKT DOSTĘPOWY Z WIELOMA RÓŻNYMI KONTROLAMI DOSTĘPU	X
WABIK	HUNY

Rys. 6.2. Propozycja znaków naznaczonego dostępu

6.2 Wardriving

Rys. 6.3. Przykład wardriving'u

Termin wardriving określa przede wszystkim techniki namierzania sieci bezprzewodowych, najczęściej z wykorzystaniem do tego celu samochodu. Jako narzędzi używa się laptopa wyposażonego w kartę Wi-Fi, antenę wzmacniającą oraz odpowiednie oprogramowanie. Metoda ta wiąże się nierozerwalnie z techniką warchalkingu, czyli oznaczania ścian budynków lub chodników w miejscach, gdzie rozpoznany został otwarty punkt dostępowy.

Popularnym programem używanym przez amatorów rozpoczynających swą przygodę z wardriving jest Netstumbler wykorzystujący metody wykrywania za pomocą skanowania aktywnego. Polega ona na oczekiwaniu odpowiedzi w postaci ramek Probe Response, na uprzednio wysłane ramki Probe Request. Dzięki nim uzyskuje się takie informacje, jak identyfikator ESSID, numer kanału, oraz dotyczące mechanizmów WEP, natężenia ruchu i prędkości. Ta metoda jest możliwa jedynie do zastosowania w sieciach otwartych, sieci zamknięte bowiem nie odpowiadają na takie zapytania, a jej funkcjonalność może zostać znacznie ograniczona przez administratora sieci, który stosuje filtrowanie ramek niosących identyfikator ESSID. Oprócz tego użycie narzędzi tego typu jest ograniczone z powodu wymogu fizycznej obecności w obrębie zasięgu nadawania karty. Programy, takie jak Netstumbler, nie analizują również ruchu sieciowego, rejestrują jedynie ruch ramek odpowiedzi, co powoduje łatwość wykrycia osoby, która posługuje się tym programem. Znacznie częściej są używane programy działające w trybie monitorowania sieci, takie jak Kismet, Airtraf, WifiScanner czy Wellenreiter.

Literatura

1. Engst A., Fleishman G., *Sieci bezprzewodowe. Praktyczny podręcznik*, Helion, Gliwice 2005
2. Krysiak K., *Sieci komputerowe. Kompendium*, Helion, Gliwice 2005
3. Ross J., *Sieci bezprzewodowe. Przewodnik po sieciach Wi-Fi i szerokopasmowych sieciach bezprzewodowych*, Wydanie II, Helion, Gliwice 2009