Bezprzewodowe połączenia sieciowe

Autor: Krzysztof Przybyłek IV FDS

Spis treści

Wstęp

Bezprzewodowa sieć (WLAN) jest elastycznym systemem komunikacji zaprojektowanym jako rozwiązanie alternatywne lub uzupełniające dla tradycyjnej sieci kablowej. Wykorzystując częstotliwości radiowe bądź podczerwone, sieć bezprzewodowa wysyła i odbiera dane minimalizując konieczność użycia połączeń kablowych. Tak więc sieć bezprzewodowa łączy w sobie transmisję danych z mobilnością użytkownika.
Sieci bezprzewodowe zyskały dużą popularność w wielu segmentach rynku jak: medycyna, handel, produkcja, magazynowanie. Użytkownicy sieci bezprzewodowych zyskują na wydajności, używając przenośnych terminali i komputerów do komunikacji z centralą siecią firmy.
Dzięki sieci bezprzewodowej użytkownik może uzyskać dostęp do informacji bez poszukiwania miejsca z dostępem do sieci, a administratorzy sieci mogą konfigurować sieć bez instalowania czy przenoszenia struktury kablowej.
Bezkonkurencyjne zalety sieci bezprzewodowej to:
- Przenośność
- Szybkość i prostota instalacji
- Elastyczność instalacji
- Redukcja kosztów eksploatacji
- Skalowalność - łatwe dostosowanie do różnych systemów informatycznych

Sieci bezprzewodowe zapewniają identyczną funkcjonalność jak sieci kablowe, bez fizycznych ograniczeń samego kabla. Konfiguracje sieci bezprzewodowych rozciągają się od prostych topologii peer-to-peer , aż do złożonych sieci oferujących dystrybucję danych i roaming. Oprócz oferowania użytkownikowi mobilności w otoczeniu sieciowym, sieci bezprzewodowe umożliwiają przenoszenie sieci - sieć można przenosić z miejsca w miejsce razem z pracownikami jej używającymi i ich wiedzą.

W opracowaniu tym skupię się głównie na technologii WLAN (Wireless LAN), jednakże nie zapominając o innych technologiach bezprzewodowych takich jak: IrDA Bluetooth, czy HomeRF.

1. Sieci bezprzewodowe wykorzystujące częstotliwości podczerwone – standard IrDA

1.1 Ogólna charakterystyka

Transmisje cyfrowe w podczerwieni zawdzięczają swoje powstanie procesom normalizacyjnym dotyczącym pilotów sterujących odbiornikami TV i magnetowidami. IrDA (Infrared Data Association) jest protokołem transmisji w podczerwieni, a także zarazem stowarzyszeniem firm zajmujących się sprzętem z transmisją podczerwoną. Dzisiaj Forum IrDA specyfikuje trzy standardy komunikacji: IrDA – Data, IrDA – Control oraz nowy – Air (Advanced Infrared). IrDA zapewnia transmisję typu punkt – punkt na odległość do 1 m w zakresie falowym 850-900 nm. Osiągane przepływności dochodzą do 16 Mb/s, a kąt transmisji nie przekracza 30º. Po obniżeniu szybkości transmisji do 75 kb/s można komunikować się na odległość ponad 5 m. Nowy protokół Air zapewnia przesyłanie danych w konfiguracji wielopunkt – wielopunkt dzięki rozszerzeniu kąta wiązki podczerwonej do 120º i rozszerzenia zasięgu do 8 m. Teraz oferuje przepływność 4 Mb/s na odległości 4 m lub 250 kb/s po podwojeniu tego dystansu. Do stowarzyszenia IrDA należą: Acer, Ascom, Apple Computer, Compaq, Ericsson, Hewlett-Packard, Intel, Microsoft, Toshiba, Motorola, Nokia Sony i wiele wiele innych firm.

Transmisja w paśmie podczerwieni ma niewątpliwą zaletę – niski pobór energii, ale i wady: głównie jest to mały zasięg oraz konieczność widzenia się przez współpracujące urządzenia. Stosowana jest zatem głównie w sprzęcie pracującym w jednym pomieszczeniu, gdzie odległości od nadajnika do odbiornika nie przekraczają kilku metrów, a bezpośrednia widoczność jest łatwa do osiągnięcia. Pewien problem stanowić mogą inne źródła podczerwieni. Jako że promieniowanie określane przez nas jako białe światło widzialne zawiera dość szerokie spektrum fal o różnej długości, może ono zakłócać pracę odbiorników podczerwieni. Producenci podzespołów starają się zaradzić temu przez taki dobór składu chemicznego stosowanych półprzewodników, aby reagowały one w największym stopniu właśnie na podczerwień. Inna metoda polega na wykorzystaniu odpowiednich filtrów optycznych. Są to filtry zaporowe dla światła widzialnego - wykonywane jako odpowiednio barwione soczewki samych elementów (kolor czarny) lub filtry zewnętrzne, zwykle w postaci czerwonej płytki z tworzywa sztucznego, umieszczanej przed odbiornikiem. Czasem jednak (np. silne światło słoneczne) filtry te mogą okazać się niewystarczające. Kłopoty może też spowodować wzajemne zakłócanie się większej liczby nadajników pracujących jednocześnie w jednym pomieszczeniu. Teoretycznie zapobiegać temu zjawisku powinno użycie zróżnicowanych sposobów kodowania informacji w poszczególnych wyrobach lub stosowanie u standaryzowanych protokołów transmisji, pozwalających na prawidłową współpracę kilku urządzeń. W praktyce jednak bywa różnie i z pewnością powinniśmy pamiętać o wszystkich niedostatkach tej technologii, aby w razie wystąpienia problemów umieć im zaradzić.

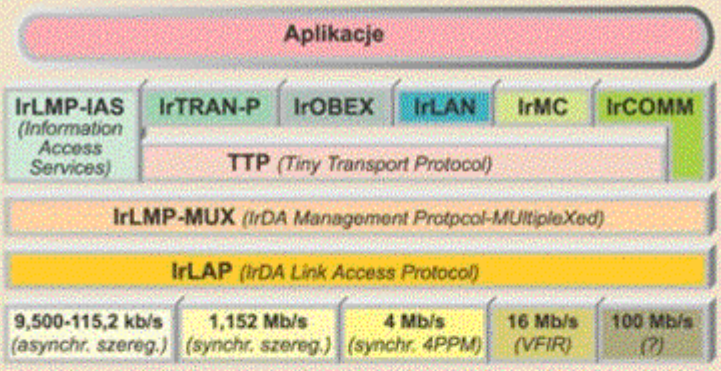
Standard ten składa się z kilku protokołów podzielonych na warstwy, korzystających wzajemnie ze swoich usług.
Jednym z protokołów jest IrCOMM, pozwalający na emulację portu szeregowego lub równoległego. Następnym jest IrLAN - protokół dostępu do sieci LAN, który umożliwia:

- dołączenie komputera do sieci LAN poprzez urządzenie dostępowe - popularne np. w Japonii;
- połączenie do sieci LAN poprzez inny komputer już połączony - w tym przypadku oba komputery współdzielą adres MAC, komputer połączony za pomocą IrLAN jest widziany wtedy jako zasób na komputerze stacjonarnym;

- utworzenie sieci LAN z dwóch komputerów łączących się ze sobą.

Są jeszcze protokoły: IrOBEX - do wymiany plików, TinyTP - zapewniający niezawodność transmisji. Wymienione protokoły, istotne z punktu widzenia użytkownika, są nieobowiązkowe i implementuje się je zależnie od potrzeb, co pozwala zmniejszyć koszty rozwiązań.

1.2 Szkic architektury IrDA



Szkic ten dobrze przystaje do rzeczywistości, chociaż do oznaczania szybkości wersji IrDA stosuje się czasami następujące nazwy:
SIR (Serial InfraRed): 2,4-115,2 kb/s;
MIR (Medium InfraRed): 0,576 i 1,15 Mb/s;
FIR (Fast InfraRed): 1,15-4 Mb/s;
VFIR (Very Fast InfraRed): 16 Mb/s.

Nazwa MIR jest nieoficjalna. W styczniu lub lutym 2002 dojdzie kolejna nazw dla oznaczania szybkości do 100 Mb/s. IrDA rozwija się bardzo dynamicznie.

Najpierw protokół IrDA wyeliminował połączenie miedziane między urządzeniami oraz interfejs RS 232. Jeśli jednostka centralna komputera lub innego urządzenia miała do przesłania np. bajt danych, to magistralą równoległą był on kierowany do układu scalonego UART, skąd w postaci szeregowej i z bitami startu oraz stopu docierał do układu kodującego, modulatora i wreszcie do nadajnika sterującego diodą LED. W ten sposób wspomniany bajt był wypromieniowany w stronę odbiornika. Tu następował proces odwrotny: przez diodę PIN i wzmacniacz wejściowy sygnał trafiał do demodulatora, dekodera i układu UART, skąd już w postaci równoległej docierał do procesora. Asynchroniczny UART przetwarza jednak z szybkością 2,4-115,2 kb/s.

Przy większych szybkościach stosuje się bardziej wydajne sterowniki komunikacyjne. Ponadto przy 16 Mb/s i wyższych szybkościach musi być zmodyfikowana warstwa IrLAP. Stąd jej wielobarwność.

1.3 IrDa w praktyce

„Irdę” można wykorzystać do łączenia z telefonem komórkowym, laptopem, drukarką, lub inną irdą. W praktyce z każdym urządzeniem, które posiada podczerwień. Ciekawym rozwiązaniem jest korzystanie z telefonu komórkowego jako modemu do Internetu o ile producent od komórki dostarczył sterowniki, aby telefon służył jako modem. Irdę podłączamy do znalezionego na płycie głównej pięcio-pinowego złącza IR.
Skąd wzięła się tak duża popularność tej technologii komunikacji? Przyczynił się do tego niski koszt produkcji przy stosunkowo dużych zaletach tego rozwiązania. IrDA z półtora metrowym kabelkiem i śledziem do PC kosztuje ok. 85 zł. Także dynamiczny rozwój rynku komputerów przenośnych, z jakimi mamy do czynienia w ostatnim czasie miał poważny udział w popularyzacji komunikacji przy użyciu podczerwieni.

Rys.1 IrDA z 1,5 m kabelkiem i śledziem

Rys.2 Przykład podłączenia telefonu komórkowego bądź PC za pomocą IrDA z laptopem

2. Sieci Bluetooth

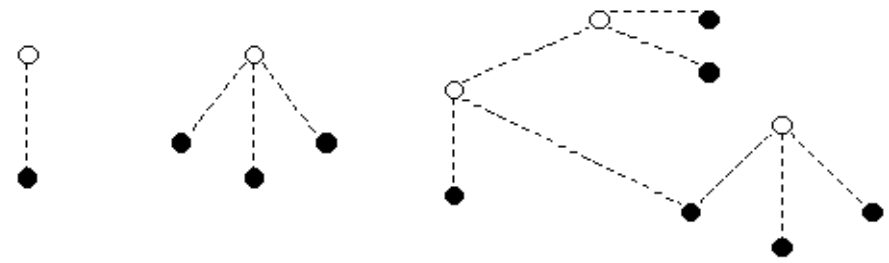
2.1 Charakterystyka ogólna

Bluetooth, opracowany przez Ericsson Mobile Communication AB, ma stać się wygodnym i tanim rozwiązaniem komunikacyjnym dla ludzi interesu będących w ciągłym ruchu. Bluetooth wykorzystuje fale radiowe do bezprzewodowej komunikacji między laptopami, telefonami komórkowymi, drukarkami, komputerami stacjonarnymi, eliminując potrzebę okablowania współpracujących w ramach sieci komputerowej urządzeń. Umożliwia bezprzewodową, automatyczną, natychmiastową, nawiązywaną ad hoc i przebiegającą w tle komunikację między poszczególnymi urządzeniami w sieci.
Prace nad Bluetooth rozpoczęto w 1994, a w 1997 Nokia, IBM, Toshiba i Intel poparły działania Ericssona, tworząc grupę Bluetooth SIG (Special Interest Group), która obecnie skupia ponad 500 firm z całego świata. SIG zdefiniował swoją technologię jako:
- zdolną do przenoszenia informacji głosowej i danych cyfrowych,
- zdolną do pracy globalnej,
- zdolną do ustalania połączenia ad hoc,
- zajmującą po zainstalowaniu jej w urządzeniu bardzo mało miejsca,
- zużywającą bardzo mało energii,
- otwarty standard,
- ogólnie dostępną.

Zastosowania Bluetooth są prawie nieograniczone. Przede wszystkim standard ten posłuży do wymiany informacji pomiędzy komputerami przenośnymi i stacjonarnymi oraz telefonami komórkowymi. Może się też pojawić się wiele rozwiązań nieprofesjonalnych : bezprzewodowe słuchawki do telefonów czy sprzętu hi-fi, zestawy głośno mówiące wbudowane w radia samochodowe, uaktywniane od razu po wejściu do pojazdu czy rozbudowane zegarki automatycznie synchronizujące dane z programem terminarza w pececie, gdy tylko znajdziemy się blisko komputera. Duże udogodnienia mogą pojawić się również w dziedzinie inteligentnego budownictwa - aktywne identyfikatory osobiste wymieniające informacje z odpowiednimi urządzeniami systemów kontroli dostępu, ochrony przeciwpożarowej, HVAC, itd., mogą uczynić pobyt w budynku przyjemniejszym i bardziej bezpiecznym.

Technologia Bluetooth do transmisji sygnałów wykorzystuje ogólnodostępne, zwolnione od licencji pasmo radiowe 2,45 GHz. Sygnał jest przenoszony na zmieniających się skokowo częstotliwościach, (1600 zmian częstotliwości na sekundę). Każdy pakiet danych przenoszony jest na innej częstotliwości, dzięki czemu zminimalizowano zakłócenia i zanikanie sygnału. Transmisja z podziałem czasu przebiega w trybie full-duplex. W promieniu od 10cm do 10m dane przekazywane są z prędkością 1 Mbit/s, ale zasięg nadajnika może być łatwo zwiększony do 100m poprzez zwiększanie jego mocy. Planuje się, że druga generacja urządzeń będzie mogła transmitować dane z prędkością do 10 Mbit/s. Bluetooth umożliwia zarówno asynchroniczną, jak i synchroniczną transmisję danych. Możliwe jest wykorzystanie asynchronicznego kanału transmisyjnego, do trzech kanałów synchronicznej, jednoczesnej transmisji mowy lub kanału asynchronicznie przesyłającego dane i synchronicznie mowę. Każdy kanał synchroniczny transmitujący głos ma przepustowość 64 kbit/s. Przepustowość asynchronicznego kanału wynosi maksymalnie 721 kbit/s w dowolnym kierunku i 57,6 kbit/s w przeciwnym kierunku lub 432,6 kbit/s w obu kierunkach. Zaimplementowanie protokołu IP wydaje się w takich warunkach bardzo proste.

Urządzenia Bluetooth mogą tworzyć dowolne zestawy tworząc tzw. *piconet* (rys.3).



Rys.3 Piconet i scatternet

A – pojedyncze połączenie master-slave

B – połączenie w trybie jeden master wiele slave'ów

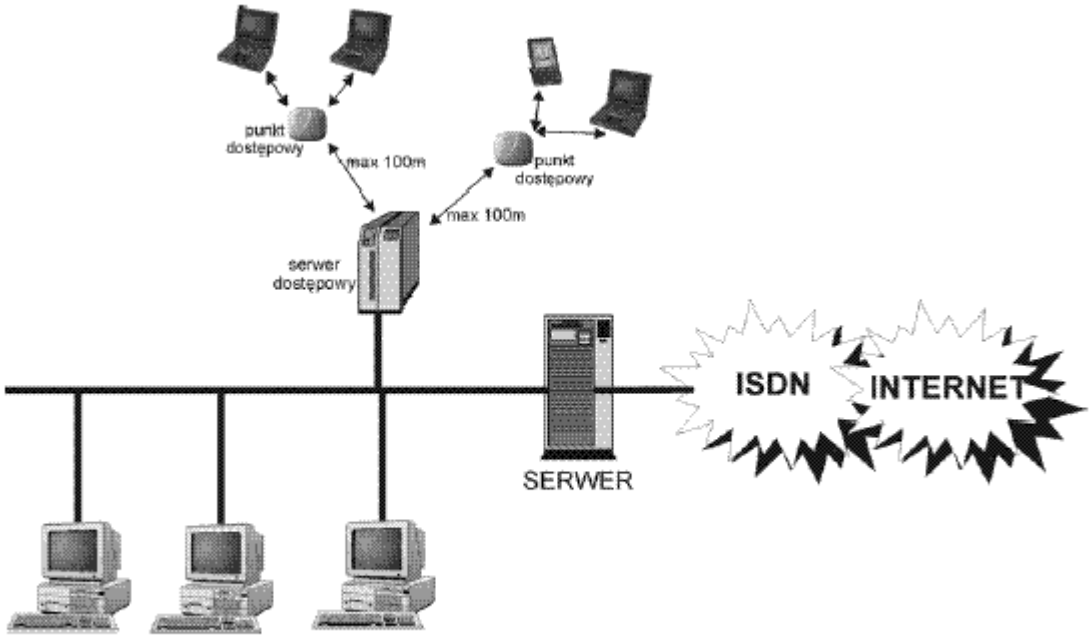
C – połączenie kilku pikosieci w scatternet

● - slave

○ - master

W skład takiej struktury wchodzi maksymalnie 8 jednostek, które mogą komunikować się każda z każdą. Jedno z urządzeń w strukturze pełni rolę nadrzędną - master (pozostałe mają status slave), określając przedziały czasu i sekwencje przydziału częstotliwości, na których komunikują się wszystkie urządzenia ze sobą. Każde z urządzeń może być w jednym z kilku stanów: aktywny (active), "snu" (standby), oczekiwania (hold), nasłuchiwania (sniff), zatrzymania (park). Na początku wszystkie urządzenia są w stanie "snu", "budząc się" co 1,28s i czekając na połączenie z jakimś urządzeniem w strukturze piconet. Urządzenie master może ustawić podrzędne jednostki w stan oczekiwania w celu zaoszczędzenia energii w momencie braku aktywności sieci. Podrzędne urządzenie może się również domagać przejścia w stan oczekiwania. W stanie nasłuchiwania urządzenia podrzędne (slave) śledzą aktywność w sieci przy zmniejszonym poborze mocy. Stan zatrzymania również ustawia dane urządzenie w tryb ograniczonego poboru mocy, zachowując jednocześnie zdolność synchronizacji z siecią, ale nie biorąc aktywnego udziału w ruchu w sieci oraz zwalniając swój adres MAC. Grupa piconet'ów pracujących niezależnie od siebie i nie będących ze sobą zsynchronizowanych tworzy strukturę nazwaną scatternet. Takie rozwiązanie pozwala na utworzenie wielu małych podsieci. Każdy piconet ma przepustowość do 1 Mbit/s, wykorzystując strukturę scatternet możliwe jest sumowanie przepustowości pojedynczych podsieci. Testy wykazały, że w sieci złożonej z 10 podsieci (piconet) redukcja prędkości jest mniejsza niż 10% z powodu kolizji. W rezultacie potencjalna przepustowość całej takiej sieci wynosi około 9 Mbit/s. Komunikacja z nowymi urządzeniami jest nawiązywana automatycznie, gdy tylko znajdą się w zasięgu dowolnego elementu sieci piconet. Mały zasięg urządzeń pracujących z Bluetooth minimalizuje możliwość zakłóceń w eterze, a dodatkowo system został zoptymalizowany pod tym kątem. Polega to na tym, że dane są transmitowane w pakietach, które są nadawane i odbierane na innych częstotliwościach. Pasmo częstotliwości dzieli się na kilka kanałów, z których każdy dzielony jest na szczeliny czasowe po 625ms każda, a podczas połączenia kanał zmienia się 1600 razy na sekundę. Ta metoda nadawania nosi nazwę Ferquency Hopping Spread Sprectum (FHSS), co tłumaczy się jako rozpraszanie widma sygnału z przeskokiem częstotliwości. W pewnej części metoda FHSS eliminuje także możliwość podsłuchiwania sygnału przez nieuprawnione osoby, co z pewnością poszerzy grono entuzjastów bezpiecznej transmisji danych. Dodatkowo w architekturę Bluetooth wbudowane są mechanizmy potwierdzania autentyczności i

szyfrowania, wskutek czego urządzenia będą mogły się komunikować tylko z tymi urządzeniami, które wskaże użytkownik.



Rys.4. Przykad połączenia sieci Bluetooth z siecią kablową z dostępem do internetu

Jak widać na rys.4, system Bluetooth składa się z serwera dostępowego, służącego do utrzymania oraz zarządzania całą infrastruktura sieci Bluetooth, ustalającego połączenia z i pomiędzy oddalonymi od siebie urządzeniami, takimi jak komputery stacjonarne, przenośne, terminale PDA oraz telefony komórkowe. Serwer dostępowy, pełniący funkcję zarządzającą wszystkimi urządzeniami Bluetooth – włączając punkty dostępowe oraz końcowe – pozwala na swobodne przemieszczanie się użytkownika pomiędzy punktami dostępowymi, dzięki czemu nie musimy przerywać połączenia z internetem nawet, kiedy przemieszczamy się np. po biurze. Dostęp do takiej sieci może być odpowiednio konfigurowany przez administratora, aby uniemożliwić wgląd np. do baz danych firmy osobom niepowołanym.

Kolejnym elementem systemu Bluetooth są punkty dostępowe, których głównym zadaniem jest zwiększenie obszaru pokrycia serwera dostępowego. Umożliwiają one użytkownikom urządzeń przenośnych na korzystanie z usług intranetowych oraz internetowych, a ich zaletą jest łatwość instalacji oraz sterowania przez serwer Bluetooth. Najczęściej stosowanymi nadajnikami zarówno w przypadku serwerów jak i punktów dostępowych są układy klasy 1, które oferują zasięg do 100m.

Ostatnimi elementami sieci są urządzenia końcowe, czyli komputery stacjonarne, laptopy, PDA, czy telefony komórkowe, wyposażone w odpowiednie adaptery Bluetooth, umożliwiającymi komunikację z innymi urządzeniami tego standardu.

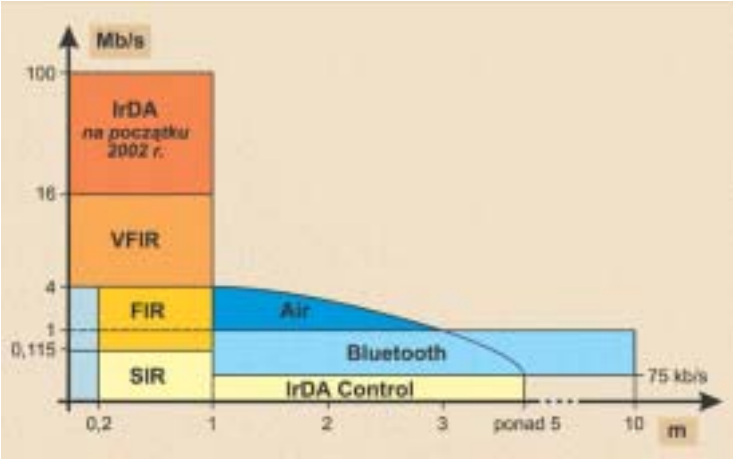
2.2 Bluetooth w praktyce

Rys. 5 Bluetooth USB adapter - umożliwia bezprzewodowe łączenie z Dial up lub siecią LAN : połączenie Internetowe lub przyłączenie do sieci LAN z urządzeniem odbiorczym (np. poprzez telefony komórkowe GSM, GPRS, CDMA lub poprzez punkt dostępowy Bluetooth LAN), Cena: 449 zł

Rys.6 Kontroler umożliwia przesyłanie danych na odległość do 100 metrów przy przepustowości do 1 Mbit/s.

2.3 IrDA kontra Bluetooth.

	Bluetooth	IrDA
Częstotliwość	2400-2483,5 MHz Hiszpania - 2445-2475 MHz Francja - 2446,5-2483,5 MHz	podczerwień 0,85-0,9 mmvv
Typ połączenia	punkt-punkt lub punkt-wielepunktów	punkt-punkt
Liczba kanałów	3 do transmisji mowy + 1 do transmisji danych/pikonet lub pojedynczy kanał/pikonet	1 do transmisji mowy lub danych
Prędkość transmisji	1 Mb/s, w przygotowaniu 10Mb/s	115.2 kbit/s, 4Mbit/s Fast Infrared (FIR),Air 16Mb/s
Zasięg	10m (można zwiększyć do 100m przy pomocy opcjonalnego wzmacniacza)	1m – 8m maksymalnie
Typ transmisji	Urządzenia podczas transmisji nie muszą się widzieć	urządzenia muszą się widzieć, wiązka o kącie transmisji 30^o
Maksymalna liczba aktywnych urządzeń	8/połączenie (pikonet), 10 pikonetów w zasięgu transmisji	2/połączenie
Multipleksacja	Kodowa	przestrzenna
Bezpieczeństwo na poziomie łącza	kodowanie + weryfikacja	Brak



Rys.7 Szybkośc Bluetooth'a na tle wszystkich wersji IrDA

Jak widać z tych charakterystyk, Bluetooth zyskuje na zasięgu (do 10 a nawet ostatnio 100 m) i bezpieczeństwie, po za tym jest widzialny przez ściany, natomiast IrDA ma większy transfer i jest znacznie tańszy. Oba standardy przeznaczone były z góry do łączenia urządzeń

peryferyjnych, jednakże Bluetooth wychodzi ponad to i służy do budowania sieci LAN na podstawie Bluetooth.

Standard Bluetooth powoli staje się jednym z najważniejszych standardów bezprzewodowych choć daleko mu jeszcze do WLAN 802.11b jeśli chodzi o jego szybkość transmisji (11 Mb/s czy nawet 54Mb/s kontra 720 kb/s), ale ciągle spadająca cena Bluetooth i opracowywana nowa specyfikacja Bluetooth 2.0 z szybkością 10Mb/s zwiastuje mu wielką przyszłość.

3. Bezprzewodowe sieci LAN – WLAN (Wireless LAN) – 802.11

3.1 Charakterystyka ogólna

O ile powyżej przedstawione standardy nadają się co najwyżej do przyłączenia paru komputerów do sieci LAN, tak niżej przedstawiona technologia posiada już wszystkie funkcje realizowane przez tradycyjne sieci LAN. Oprócz typowych dla Bluetooth i IrDA sieci PAN (Personal Area Network) most bezprzewodowy WLAN oparty na standardzie IEEE 802.11 łączy już dwie przewodowe bądź bezprzewodowe sieci w dwóch oddzielnych budynkach. WLAN to elastyczny system komunikacyjny, który może służyć nie tylko do wymiany danych między komputerami przenośnymi, ale też do uzupełniania i łączenia tradycyjnych przewodowych sieci LAN czy z powodzeniem nawet do budowania niezależnych sieci WLAN. Dane są przesyłane droga radiową w trybie peer-to-peer (np. na linii PC-PC, PC-hub lub drukarka-hub) i w trybie point-to point (np. LAN-LAN). Podstawowymi elementami sieci WLAN są wbudowane karty sieciowe i punkty dostępu(mosty). Karty sieciowe zapewniają interfejs między końcowym urządzeniem użytkownika i anteną, która wysyła/odbiera dane do/z punktu dostępu. Punkty dostępu pełnią rolę nadajników/odbiorników między siecią bezprzewodową a siecią przewodową, łączy obydwie sieci umożliwiając przesyłanie danych między klientami sieci bezprzewodowej i siecią stacjonarną. Każdy taki punkt zwiększa również ogólną wydajność i zasięg systemu bezprzewodowego. Użytkownik może korzystać z roamingu (przenoszenie łączności z zachowaniem ciągłości transmisji między punktami dostępów) nie tracąc połączenia z siecią, podobnie jak w przypadku telefonów komórkowych. Urządzenie wraz z oprogramowaniem komputera służy klientom bezprzewodowym jako koncentrator telekomunikacyjny i zapewnia połączenie ze stacjonarną siecią LAN. Punkty dostępu są niezbędne do uzyskania dostępu do sieci, ale nie są potrzebne do nawiązywania połączeń typu peer-to-peer. Jednakże zainstalowanie punktów dostępu w sieci bezprzewodowej daje istotne korzyści, gdyż działają one jak repeatery zwiększając prawie dwukrotnie zasięg WLAN, w porównaniu z siecią doraźnych połączeń dwupunktowych. Pełnią tez rolę kontrolerów ruchu, sterując całą transmisją ruchu w sieci i umożliwiając klientom sieci bezprzewodowej uzyskanie maksymalnej szybkości transferu. Ponadto punkt dostępu może stanowić centralny punkt łączności ze światem zewnętrznym, zapewniając m.in. współużytkowanie połączeń z internetem.

Karty do transmisji bezprzewodowej instaluje się w stacjach roboczych, wyposażone w szynę PCI, ISA, USB bądź PCMCIA – i mają zainstalowaną jedną lub dwie anteny.

Mosty bezprzewodowe spełniają te same funkcje co punkty dostępu, ale mają więcej kanałów i zapewniają szersze pasmo służące do łączenia przewodowych segmentów sieci lokalnej z segmentami bezprzewodowymi. Most może być także używany do łączenia dwóch budynków. W takim przypadku urządzenia z anteną w kształcie spodka instaluje się na dachach tych budynków.

Rys.9 Wykorzystanie sieci bezprzewodowej w przypadku braku "Acces Point'a".

Rys.10 Połączenie dwóch odrębnych podsieci, w tym przypadku są to sieci przewodowe. W celu polepszenia jakości transmisji stosuje się zamianę małych anten przystosowanych do transmisji wewnątrz budynku na zewnętrzne anteny kierunkowe. Możemy w ten sposób połączyć np. dwa budynki.

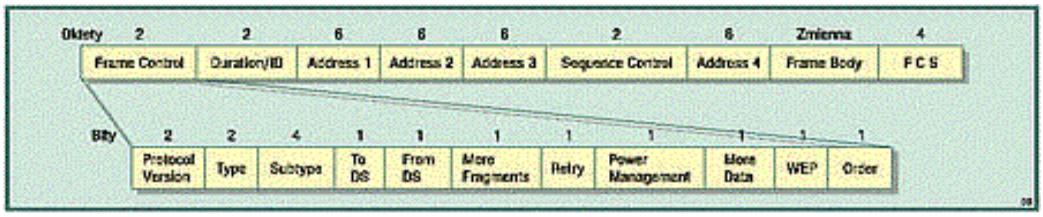
Rys.8 Punkt dostępowy jest tu podłączony do sieci kablowej, posiada dostęp zarówno do serwera, innych użytkowników jak i internetu. Każdy punkt dostępowy może obsłużyć wielu użytkowników. Ich dokładna liczba zależy od ilości i rodzaju transmitowanych danych. Przyjmuje się że jeden punkt dostępowy bezproblemowo obsługuje od 15 do 50 użytkowników. Zasięg działanie dwóch urządzeń sieci bezprzewodowej wewnątrz budynków to około 300 metrów.

Rys. 11 Tak schematycznie wyglądają trzy klasyczne (kablowe) sieci lokalne połączone łączem bezprzewodowym.

3.2 Zasada pracy sieci WLAN

Fale radiowe są często określane jako nośnik radiowy, ponieważ pełnią proste zadanie – dostarczają energię do odległego odbiornika. Transmitowane dane są nakładane na nośną radiową, tak aby mogły być dokładnie wyodrębnione przez stację końcową. Proces ten jest nazywany jako modulacja nośnej przez transmitowaną informację. Gdy dane zostaną nałożone na nośna radiową, sygnał radiowy zajmuje więcej niż pojedynczą częstotliwość, ponieważ częstotliwość lub szybkość bitowa zmodulowanej informacji dodaje się do nośnej. Jeśli fale radiowe są transmitowane w tym samym obszarze na różnych częstotliwościach, w tym samym czasie możemy mieć do czynienia z wieloma nośnymi radiowymi, a żadna z nich nie zakłóca pozostałych nośnych. Aby wyodrębnić dane, odbiornik wybiera jedną częstotliwość odrzucając wszystkie inne sygnały na innych częstotliwościach. W typowej konfiguracji WLAN punkt dostępu łączy się z siecią kablową, używając standardowego okablowania ethernetowego. Punkt dostępu odbiera, buforuje i transmituje dane między siecią WLAN a siecią kablową. Pojedynczy punkt dostępu może obsługiwać niewielką grupę użytkowników i może wysyłać sygnały na odległość 30 – 500 m. Użytkownicy końcowi uzyskują dostęp do sieci WLAN za pomocą bezprzewodowych adapterów LAN, które są instalowane w komputerach przenośnych lub stanowią integralną ich część. Adaptery WLAN pełnią funkcję interfejsu między sieciowym systemem operacyjnym klienta a falami radiowymi (poprzez antenę)

Standard 802.11 specyfikuje warstwę dostępu do medium - MAC i trzy niekompatybilne ze sobą warstwy fizyczne.



Rys.12 Format ramki MAC w 802.11

Ramka warstwy dostępu do medium pokazana jest na rys.12. Pola Address 2, Address 3, Sequence Control i Address 4 występują tylko w niektórych typach ramek. Format pola Frame Control jest przedstawiony poniżej i zawiera następujące podpola:

- Protocol Version - wersja protokołu (2 bity). Urządzenie, które dostanie ramkę z wyższą wersją protokołu niż sama implementuje, wyrzuca ramkę bez powiadomienia.
- Type i Subtype - typ i podtyp ramki. Typ ramki to Zarządzanie, Kontrola, Dane i Zarezerwowane. Podtyp wskazuje na treść ramki. Przykładowe podtypy typu Kontrola to żądanie wysłania (RTS) i potwierdzenie (ACK).
- ToDS i FromDS - wskazuje na kierunek ramki z-do systemu dystrybucyjnego.
- MoreFragments - jedynka, jeżeli ramka zawiera wiadomość, której następny fragment będzie wysłany następną ramką, zero - w wypadku przeciwnym.
- Retry - jedynka, jeżeli ramka jest retransmitowana. Używane przez stację odbiorczą do eliminowania powtarzających się ramek.
- Power Management - służy do informowania punktu dostępowego o trybie pracy stacji. Jedynka w przypadku trybu oszczędnego, zero w przypadku normalnego trybu pracy. Punkt dostępowy ma wartość tego pola ustawioną zawsze na zero.
- More Data - informuje terminal będący w trybie oszczędnym, czy w buforze znajdują się ramki dla niego przeznaczone.
- WEP - jedynka, jeżeli dane zawarte w ramce zostały zaszyfrowane przez algorytm WEP.
- Order - jedynka, jeżeli dane transmitowane pochodzą z klasy StrictlyOrdered. Pole Duration/ID przenosi zwykle długość ramki. Tylko gdy ramka typu Kontrola należy do podtypu PowerSafe-Poll, przenosi informację AID.

Pole Sequence Control zawiera informacje o numerze wiadomości liczonym licznikiem modulo 4096 i kolejnym numerze fragmentu w ramach jednej wiadomości. Pole Danych może przenosić zarówno dane użytkownika, jak i pola wiadomości sterujących. W przypadku tych drugich ma ściśle zdefiniowany format dla każdego typu wiadomości.

3.3 Metody modulacji radiowej częstotliwości komunikacyjnej

Standard definiuje w warstwie fizycznej PHY trzy różne sposoby modulacji radiowej częstotliwości komunikacyjnej. Pierwszy to modulacja rozproszonego widma z bezpośrednim szeregowaniem bitów - **DSSS** (Direct Sequence Spread Spektrum). Drugi to modulacja w widmie rozproszonym ze skokową zmianą używanego kanału - **FHSS** (Frequency Hopping Spread Spectrum). Trzeci – **OFDM** (Orthogonal Frequency Division Multiplexing) . Wszystkie metody modulacji zostały zaprojektowane na potrzeby militarne by zapewnić niezawodność, integralność i bezpieczeństwo transmisji. Obydwie wykorzystują jedyne w swoim rodzaju metody transmisji danych.

W technologii **FHSS** pasmo podzielone jest na 83 kanały o szerokości 1 MHz, informacje przesyłane są przez interfejs radiowy kanałem o szerokości 5 MHz z przepustowością do 1,6 Mb/s. Częstotliwość fali nośnej zmieniana jest skokowo (frequency hopping) co kilkaset ms, transmisja w rzeczywistości przebiega w prawie całym paśmie 2,4-2,5 GHz, co chwilę na innej częstotliwości. Jeśli na pewnej częstotliwości występują zakłócenia lub interferencje fal uniemożliwiające komunikację, przesyłanie danych jest kontynuowane po następnym skoku, na innej częstotliwości. FHSS jest przede wszystkim odporny na zakłócenia, doskonale nadaje się do wykorzystania w środowiskach przemysłowych czy zastosowaniach militarnych, gdzie ciągłe zmiany częstotliwości fali nośnej utrudniają podsłuchanie sygnału. Może być jednak wykorzystany tam, gdzie nie jest potrzebna duża przepustowość (1,6 Mb/s w łączu internetowym czy zastosowaniach logistycznych przeważnie wystarcza, natomiast w typowej, biurowej sieci LAN jest z reguły zbyt mała). Jedną z zalet FHSS jest możliwość pracy we wspólnym paśmie wielu sieci, występujących na jednym terenie, bez wzajemnego zakłócania się.

DSSS oferuje znacznie więcej. Obecne rozwiązania, zgodne ze standardem IEEE 802.11b, pracują z szybkością 11 Mb/s. Podstawowa różnica w działaniu sieci polega na tym, że w DSSS pasmo 2,4-2,5 GHz jest dzielone na kilkanaście kanałów (w Europie można używać kanałów z zakresu 1-13), komunikacja pomiędzy dwoma urządzeniami odbywa się na jednym z tych kanałów. Ponieważ kanały te są dość szerokie, wydajność takiej sieci jest znacznie większa. Jednak aby kanały nie zachodziły na siebie, odległość między ich centrami powinna wynosić przynajmniej 25 MHz. Warunek ten spełniają kanały 1, 6 i 11 o częstotliwościach 2412, 2437 i 2462 MHz (lub podobne kombinacje, np. 2, 7, 12). W praktyce dostępna liczba kanałów nie może więc być wykorzystana, co jest wadą DSSS.
Należy jednak pamiętać, że przepustowość sieci wykorzystujących DSSS, która wynosi nominalnie 11 Mb/s, w rzeczywistości jest znacznie mniejsza. Przez bardzo szerokie pasmo (prawie trzecią część całego pasma 2,4-2,5 GHz) przesyłane są nie tylko dane użytkownika, ale także mnóstwo nadmiarowych informacji, dzięki którym zapewniona jest niezawodna transmisja danych, ale dzieje się to kosztem wydajności.

Modulacja **OFDM** została tak zoptymalizowana, aby interfejs bezprzewodowy mógł transmitować dane w środowiskach pełnych zakłóceń, takich jak zatłoczone obszary miejskie, czy nowy dostęp do internetu poprzez gniazdka elektryczne. Udostępnia 8 kanałów 20-megahercowych z możliwością ich przełączania. Dlatego OFDM pracuje niezawodnie i nie ma tych ograniczeń i wad (chodzi o odległość, odporność na zakłócenia, łatwość instalowania i rozmiary anteny), które towarzyszą innym systemom łączności bezprzewodowej.

Wiele sieci WLAN opartych na standardzie 802.11 korzysta z techniki FHSS, która jest nie tylko stosunkowo tania, ale także wyróżnia się niewielkim zużyciem energii stosowanych urządzeń. Skomplikowany mechanizm zarządzania skokami częstotliwości obniża jednak szybkość transmisji danych i utrudnia roamingi. Z tego też względu systemy 802.11b wykorzystują technikę DSSS, która zapewnia szybką transmisję danych nawet na duże odległości.

3.4 Standardy WLAN

3.4.1 Rodzina standardów IEEE 802.11

802.11 to cała rodzina specyfikacji zaakceptowana przez IEEE w 1997r. Definiuje sposób transmitowania danych za pomocą fal radiowych między bezprzewodowym klientem a stacją bazową lub między dwoma bezprzewodowymi

klientami. Operuje na dwóch najniższych warstwach OSI – fizycznej i łącza danych. W skład standardu 802.11 wchodzą:

1. Specyfikacja 802.11 – opisuje działanie sieci WLAN przesyłających dane z szybkością 1 lub 2 Mb/s, używając częstotliwości 2,4 GHz i metod modulacji FHSS lub DSSS. Wraz z rosnącą popularnością przekazu głosu i obrazu przez sieci danych, coraz głośniejsza stawała się krytyka standardu 802.11 za niewystarczającą jakość transmisji w stanie wysokiego obciążenia sieci.
2. Specyfikacja 802.11b – (określana też jako 802.11 High Rate lub Wi-Fi), opisuje działanie sieci WLAN przesyłających dane z szybkością 11 Mb/s (z możliwością przechodzenia na niższe szybkości: 5,5, 2 lub 1Mb/s), wykorzystując częstotliwość 2,4 GHz. Używa tylko techniki DSSS i była ratyfikowana w 1999r.
3. Specyfikacja 802.11a (Wi-Fi 5)– opisuje działanie sieci WLAN przesyłających dane z szybkością 54 Mb/s, wykorzystując częstotliwość 5 GHz. 802.11a używa techniki kodowania OFDM. Ma dwie podstawowe zalety w porównaniu ze standardem 802.11b:szybkość i liczba nie zachodzących na siebie kanałów – osiem. W przypadku częstotliwości 2,4 GHz są to tylko trzy kanały. Ogólna szerokość pasma jest też większa niż przy 2,4GHz – przy 2,4 jest to 83,5 MHz, a przy 5 – 300MHz. Ponieważ oba standardy pracują na innych częstotliwościach, nie są one zgodne ze sobą. Punkt dostępu 2,4 GHz nie może współpracować z karta sieciową 5 GHZ. Jednak oba standardy mogą być stosowane w tym samym systemie informatycznym. Użytkownicy 802.11a i b mogą korzystać z różnych punktów dostępu, które są podłączone do tej samej sieci LAN. Wyższa częstotliwość używana przez 802.11a oznacza mniejszy zasięg, dlatego konieczne jest stosowanie większej ilości punktów dostępu niż w przypadku 802.11b. Jednak pracują ok. trzy razy wydajniej, ale też są o ok. 30 % droższe od 802.11b. W Europie standard nie przyjął się gdyż częstotliwość 5 GHz jest zarezerwowana dla standardu HiperLAN.
4. Specyfikacja 802.11g (jeszcze nie zaaprobowana) – opisuje działanie sieci WLAN pracujących z szybkością od 11 do 54 Mb/s z wykorzystaniem częstotliwości 2,4 GHz a więc przy trzech możliwych kanałach, z wykorzystaniem modulacji DSSS. Odznacza się mniejszym poborem mocy, większym zasięgiem i szybkością oraz lepszym wskaźnikiem penetracji niż 802.11a, a co najważniejsze jest zgodna z 802.11b. W przypadku topologii, gdzie gęstość rozlokowania punktów dostępu jest mała, a przeszkody i dystans są dosyć znaczne, 802.11g oferuje większą przepływność niż 802.11a. Standard przewiduje też możliwość stosowania modulacji OFDM/CCK, zwiększając tym samym efektywność pracy.

Najważniejsze obecnie rozwijane standardy to:

- 802.11h - zapewnienie lepszych mechanizmów transmisji radiowej poprzez dynamiczny przydział kanałów radiowych i kontrolę mocy,
- 802.11j - zapewnienie w przyszłości globalnego standardu zgodnego z IEEE, ETSI Hiprelan 2,
- 802.11d - zdefiniowanie takich parametrów użytkowych i wymogów, aby 802.11 mógł być używany w innych krajach (poza USA),
- 802.11e - definiuje zarządzanie jakością usług QoS,
- 802.11i - obejmuje rozszerzenie i polepszenie mechanizmów bezpieczeństwa i autoryzacji użytkowników sieci,
- 802.11f - grupa zajmująca się rozwojem protokołu IAPP (Inter-Access Point Protocol) służącego do roamingu w sieciach 802.11.

Porównanie standardów

Standardy IEEE WLAN	802.11	802.11a	802.11b	802.11g
Data akceptacji standardu	Lipiec 1997	Wrzesień 1999	Wrzesień 1997	Faza „draft" ma być ukończona na początku 2003r.
Dostępna szerokość pasma (MHz)	83,5	300	83,5	83,5
Częstotliwość (GHz) i metoda modulacji	2,4 – 2,4835 DSSS, FHSS	5,15 – 5,35 OFDM 5,725 – 5,825 OFDM	2,4 – 2,4835 DSSS	2,4 – 2,4835 DSSS, OFDM
Liczba nie zachodzących na siebie kanałów	3 (w sieciach zewnętrznych / wewnętrznych)	4 w sieciach wewnętrznych (pasmo UNII1) 4 w sieciach wewnętrznych / zewnętrznych (pasmo UNII2) 4 w sieciach zewnętrznych (pasmo UNII3)	3 (w sieciach zewnętrznych / wewnętrznych)	3 (w sieciach zewnętrznych / wewnętrznych)
Szybkość przesyłania danych na kanał (Mb/s)	2,1	54; 48; 36; 24; 18; 12; 9; 6	11; 5,5; 2,1	54; 36; 33; 24; 22; 12; 11; 9; 6; 5,5; 2
Zgodność ze specyfikacją	802.11	Wi-Fi5	Wi-Fi	Na razie brak zgodności

3.4.2 HiperLAN1, HiperLAN2

HiperLAN (ang. High Performance Radio Local Area Network - Wysoka Jakość Radiowa w Sieciach Lokalnych) jest europejskim standardem transmisji radiowej opracowanym przez ETSI (ang. European Telecomunication Standard Institute - Europejski Instytut Normalizacyjny do Spraw Telekomunikacji). Prędkość transmisji wynosi do 20Mb/s (zasięg 50m) oraz 11Mb/s (zasięg 100m). Zasięg transmisji można zwiększyć do 800m jednak przepustowość spada do 1Mb/s. Obecnie funkcjonują dwa rodzaje tego standardu, a mianowicie HiperLAN 1 oraz HiperLAN 2. HiperLAN 1 umożliwia pracę w paśmie 5,3GHz z prędkością 23,5Mb/s. Jest to technologia typu plug and play nie wymagająca konfigurowania sieci. Natomiast HiperLAN 2 jest standardem bezprzewodowego ATM (ang. Asynchronous Transfer Mode - asynchroniczny tryb przenoszenia) i dobrze funkcjonuje jako sieć dostępowa do sieci UMTS (ang. Universal Mobile Telecommunication System - Uniwersalny

System Telekomunikacji Ruchomej). Używa technologii OFDM i TDMA(Time Division Multiple Access). Główna zaleta tego standardu polega na tym, że może on zagwarantować wybranym użytkownikom określoną przepustowość

3.4.3 RadioLAN – bez standardów ale wydajnie

RadioLAN to bezprzewodowa sieć LAN, która pracuje wyjątkowo wydajnie, ale nie spełnia wymagań stawianych przez IEEE 802.11. RadioLAN wykorzystuje nietypową częstotliwość 5,8 GHz i może przesyłać pakiety z szybkością (teoretycznie) 10 Mb/s, czyli pięć razy szybciej niż sieci oparte na 802.11. Sieć ta w praktyce nie pracuje aż tak szybko, ale w odległości 1,5 m (notebook – punkt dostępu) osiąga rzeczywiście przepustowość 4,39 Mb/s. Po ustawieniu notebooka w odległości 11m przepustowość spada do 1,88 Mb/s, przy czym tylko 30% ramek jest wtedy przesyłana od razu bezbłędnie. Technologia RadioLAN zakłada stosowanie bardzo dużych anten. Wystarczy by ustawić antenę pod nieco innym kątem, a przepustowość od razu ulega zmianie. Po mimo stosowania tak dużych anten maksymalny zakres tej sieci wynosi 20 m. Dlatego rozwiązanie to nie nadaje się do implementowania w dużych budynkach, chyba że zdecydujemy się na instalowanie wielu punktów dostępu, ale to kosztuje. Sieć ma jedną podstawową zaletę: duża przepustowość przy niewielkim oddaleniu od notebooka punktu dostępu, oraz wadę: niewielki zasięg. Jeśli więc biuro jest niewielkie, a przepustowość sieci gra pierwszoplanową rolę, może to być dobre rozwiązanie (pomijając brak zgodności)

3.5 Bezpieczeństwo sieci WLAN

Sieci bezprzewodowe oferują dużo mniejszy stopień ochrony przed włamaniem i podsłuchem. Teoretycznie chronić ma ją parę specjalnie do tego celu stworzonych protokołów.

Protokół **WEP** (Wired Equivalent Privacy) – jest to protokół bezpieczeństwa wchodzący w skład standardu 802.11b. Zapewnia bezpieczeństwo szyfrując dane przesyłane drogą radiową. Jednak ponieważ WEP operuje na dwóch najniższych warstwach modelu OSI, nie zapewnia do końca bezpieczeństwa. Wykryto, że WEP poddany następującym atakom:

- pasywne ataki deszyfrujące ruch sieciowy bazujące na analizie statystycznej,
- aktywne ataki wstrzykujące nowy ruch generowany w nieautoryzowanej stacji ruchomej, bazujący na znanym prostym tekście,
- aktywne ataki deszyfrujące ruch sieciowy, bazujące na oszukiwaniu punktu dostępowego,
- atak "Dictionary building", podczas którego, całodniowy ruch sieciowy jest monitorowany i analizowany pozwalając na automatyczne deszyfrowanie całego ruchu w czasie rzeczywistym.

A oto słabe punkty protokołu WEP:

- Statyczne klucze – klucze WEP są stosowane w kartach instalowanych w komputerach i punktach dostępu w tej samej bezprzewodowej sieci LAN i nie są zmieniane automatycznie zgodnie z wcześniej ustalonymi zasadami. Co gorsza, standard WEP nie dopracował się metody dystrybucji kluczy. Gdy klucze zostaną skonfigurowane dla każdego użytkownika, bardzo trudno je zmienić. Administratorzy bardzo niechętnie modyfikują klucze WEP, ponieważ pociąga to za sobą konieczność dokonania zmian u końcowego użytkownika .

- Słabe szyfrowanie – grupa robocza 802.11 ograniczyła długość klucza WEP do 40 bitów. Pozwala to na ograniczony poziom szyfrowania: zabezpieczenie można łatwo złamać. Haker używający statycznych narzędzi analizy może przechwycić klucz WEP z bezprzewodowej sieci LAN w czasie krótszym niż 24 godz., a przy użyciu 250 stacji – w 4 godz.

EAP (Extensible Authentication Protocol) to protokół wspierający wiele metod uwierzytelniania., takich jak Kerberos, Token Ring, certyfikaty, klucz uwierzytelniania czy tzw. inteligentne karty (smart card). Standard IEEE 802.1x określa jak informacje EAP powinny być kapsułkowane w ramkach LAN.

Standard 802.1x potrafi dynamicznie alokować klucze szyfrowania. Protokół wymienia informacje pomiędzy dwiema stronami korzystając z usług serwera uwierzytelniania. Standard pracuje w następujący sposób:

1. Gdy klient próbuje się połączyć z punktem dostępu, do akcji wkracza protokół EAP, uzgadniając wstępne procedury.
2. Punkt dostępu wyznacza port , który będzie obsługiwać wyłącznie ruch EAP i prosi klienta o identyfikację.
3. Klient odpowiada.
4. Punkt dostępu żąda od serwera uwierzytelniania.
5. Jeśli klient zostanie uwierzytelniony, punkt dostępu zaakceptuje ruch.

Jeśli proces uwierzytelniania zakończy się sukcesem, punkt dostępu zaczyna obsługiwać inne protokoły. Gdy klient wyloguje się, punkt dostępu wyłącza porty obsługujące tego klienta. Sam protokół EAP nie definiuje wszystkich technik zabezpieczania i wymaga zaimplementowania jednej z metod uwierzytelniania, takiej jak LEAP (Lightweith Extensible Authentication Protocol) lub EAP-TLS (EAP Transport Layer Security). Obie metody są oparte na mechanizmie obupólnego uwierzytelniania między klientem a punktem dostępu. Metoda LEAP jest stosowana w sieciach WLAN Cisco, gdzie dynamicznie generuje klucze WEP. Metoda EAP-TLS wymaga, aby klienci i punkty dostępu dysponowały certyfikatami cyfrowymi, które pozwalają na dynamiczną dystrybucję kluczy WEP przez bezpieczne połączenia. Metodę EAP-TLS wspiera Windows XP oraz wielu producentów sieci WLAN. Problem z produktami 802.1x polega na tym, że używają one ciągle szyfrowania WEP, które jest stosunkowo słabe. Jednak 802.1x zmienia klucze na tyle często, że minimalizuje niebezpieczeństwo włamań. Administrator może tak skonfigurować system, aby klucze były zmienianie co parę minut, co godzinę, co tydzień lub po zakończeniu każdej sesji.

802.11i to kolejna próba zwiększenia bezpieczeństwa, przewiduje częste zmiany klucza i wzmocnienie procesu szyfrowania.

3.6 WLAN w praktyce

3.6.1 Regulacje prawne dotyczące sieci bezprzewodowej w Polsce

Sieci bezprzewodowe są regulowane w Polsce ustawą: ... Mówi ona że generalnie wykorzystywanie fal radiowych wymaga zezwolenia właściwego urzędu. Jednak w pewnych przypadkach zezwolenie takie nie jest konieczne. Jest to regulowane poprzez "Rozporządzenie Ministra Infrastruktury z dnia 6 sierpnia 2002 r. w sprawie urządzeń

radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia" poz. 1162 w Dz. Ustaw RP nr 138 z dnia 30.08.2002. W aneksie tego rozporządzenia można przeczytać iż lokalne sieci komputerowe nie wymagają zezwolenia jeśli pracują w jednym z 4 wymienionych pasm, korzystają z anten zintegrowanych bądź dołączonych oraz o ile e.i.r.p. (efektywna izotropowa moc promieniowania) nie przekracza odpowiednio:

- 100mW w paśmie 2400-2483,5 MHz
- 200mW w paśmie 5150-5350 MHz
- 1W w paśmie 5470-5725 MHz
- 100mW w paśmie 17.1-17.3 GHz

Dodatkowo wg rozporządzenia tylko pasmo 5470-5725 może być używane na zewnątrz. Korzystanie z anten zewnętrznych wymaga zawsze zezwolenia. Dodatkowo są dodatkowe warunki typu sterowanie mocą i dynamiczny przydział częstotliowści (dla 5470-5725).
W przypadku zezwolenia należy liczyć się z dużymi kosztami. Koszt rejestracji to ok. 2000 zł, drugie tyle to roczny koszt zezwolenia.

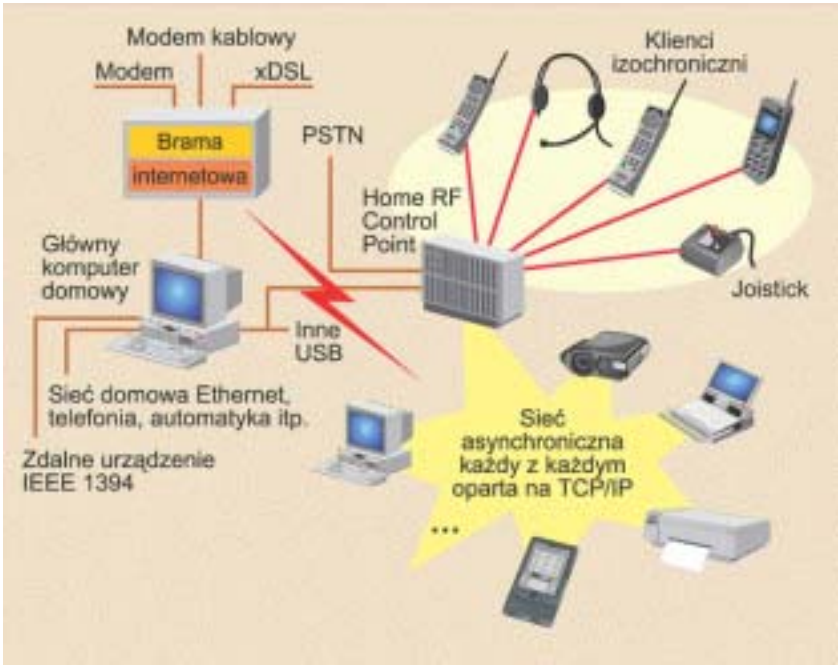
3.6.2 Koszty sprzętu

Generalnie stacja bazowa to ok. 600zl, karty USB 300-400zl. Koszt anteny zależy od jakości, mocy i kąta. Przy łączeniu dwóch bloków na odległość 100-300m można się obejść bez anten. Na odległość do 1km powinny wystarczyć najtańsze anteny panelowe po ok. 80zł. Link na odległość 2-4km wymaga anten za 200-400zł. Oczywiście sytuacja jest bardziej skomplikowana gdy nie jest to link punkt-do-punktu ale gdy do jednego punktu dostępowego (AP) podłączonych jest pary klientów - wtedy należy również wziąć pod uwagę kąt w płaszczyźnie horyzontalnej. Oczywiście anteny dookólne są droższe niż anteny kierunkowe o tym samym wzmocnieniu. Często więc opłaca się użyć jednej lub więcej anten sektorowych (nie można ich postawić obok siebie).

Sieci oparte na IEEE 802.11 jeszcze do niedawna były relatywnie bardzo kosztowne, zarówno ze względu na stopień złożoności konstrukcji jak i na stosunkowo niewielkie zainteresowanie. Obecnie, dzięki postępowi technologicznemu, urządzenia zgodne z IEEE 802.11b zyskały popularność - pojawiają się konstrukcje palmtopów i internet appliances, które wykorzystują tę technikę do komunikacji z Internetem. Oczywistą konsekwencją tego rodzaju zastosowań stało się pojawienie na rynku również rozwiązań "bazowych", takich jak np. modem kablowy czy ADSL, wyposażony w interfejs radiowy IEEE 802.11b.

4. Standard HomeRF

HomeRF to standard domowej łączności radiowej zaproponowany w 1998 r. przez HRF-WG (Home Radio Frequency-Working Group) do bezprzewodowej komunikacji między komputerami osobistymi a urządzeniami elektronicznymi powszechnego użytku. Szczególną własnością HomeRF, wyróżniającą ten protokół spośród innych norm sieciowych transmisji bezprzewodowej, jest równoczesne zapewnienie: szerokopasmowego dostęp do Internetu, współdzielenia zasobów, wielu sesji strumieni medialnych i kilku wysokiej jakości połączeń głosowych.
Użytkownicy HomeRF 2.0 mogą przesyłać głos, dane oraz strumienie audio-wideo pomiędzy różnymi produktami HomeRF służącymi do pracy i zabawy - w tym komputery PC, terminale WEB, urządzenia PDA, telefony bezprzewodowe, głośniki bezprzewodowe oraz coraz większą ilość urządzeń audio i telewizyjnych.
W HomeRF zdefiniowano najważniejszy protokół - SWAP (*Shared Wireless Access Protocol*). Obsługuje on CSMA/CA (*Carrier Sense Multiple Access/Collision Avoidance*), zbliżony do używanego w IEEE 802.11 i TDMA. SWAP jest jedną z możliwych opcji połączenia dla przyszłych sieci domowych. Relację tego ważnego protokołu z innymi urządzeniami przedstawiono na rysunku 13.



Rys.13 Wizja SWAP dla standardu HomeRF

Główny komputer osobisty w domu jest połączony z bramą, którą może być modem klasyczny, xDSL lub kablowy. Łącze może być ustalone za pośrednictwem zwykłego przewodu lub połączenia SWAP. Użytkownik komputera chce mieć lokalnie usługi i urządzenia, takie jak drukowanie, skanowanie, czytniki CD, DVD itp
Architektura SWAP łączy w sobie cechy zarządzanej sieci dostarczającej izochroniczne dane (np. głosowe) oraz sieci równorzędnej typu *peer to peer*, która zapewnia przesyłanie danych. Produkty HomeRF operują w globalnie otwartym pasmie 2,4 GHz, podobnie jak Bluetooth,

IEEE 802.11b i kuchenki mikrofalowe. W paśmie tym utratę pakietów najczęściej wywołują właśnie kuchenki mikrofalowe, chociaż mogą je zakłócać także inne sieci bezprzewodowe, jak i bezprzewodowe telefony funkcjonujące w paśmie 2,4 GHz. Stacje radiowe są dosyć proste - wymagają tych samych układów podstawowych co Bluetooth. Rozpraszają niewielką moc - ok. 10 mW.

Autorzy standardu zdawali sobie sprawę z tego, że przy tak niskich prędkościach w stosunku do konkurentów los produktów jest niepewny, a przy seryjnej produkcji 802.11 i małym zainteresowaniu HomeRF-em również przewaga cenowa będzie maleć. Oprócz tego HomeRF miał niezamierzonego konkurenta ze strony coraz popularniejszej technologii Bluetooth o niewiele niższej prędkości i zdecydowanie niższych cenach. Dla rozwiązań domowych sieć bezprzewodowa Bluetooth, współpracująca jednocześnie z PDA, aparatami cyfrowymi i telefonami komórkowymi byłaby konkurentem nie do pobicia. Dlatego właśnie powstała specyfikacja HomeRF 2.0, która pozwala na szybszą transmisję, 5 lub 10 Mb/s, wykorzystując szerszy 3,5 MHz kanał, zachowując równocześnie możliwość transmisji w dwóch wcześniejszych trybach. Planowana jest również wersja 3.0 działająca z prędkościami powyżej 20 Mb/s. Dzięki temu HomeRF ma szansę zaistnieć wśród odbiorców mniej wymagających, stając się dopiero wraz z wersją drugą technologią przejściową pomiędzy Bluetoothem a 802.11.

HomeRF jest jedyną bezprzewodową technologią sieciową zaprojektowaną całkowicie dla klienta indywidualnego, skoncentrowaną na takich aspektach jak łatwość instalacji i przystępną cenę. Tak więc produkty HomeRF są proste w użyciu, bezpieczne, niezawodne i nie drogie.

5. Podsumowanie

Zalety sieci bezprzewodowych:

- Jest prosta w montażu.
- Łatwa diagnoza usterki.
- Daje duże możliwości rozbudowy (modularność).
- Swoboda poruszania się.
- Nie wymaga okablowania.
- Można ją połączyć z kablową siecią LAN.
- Anteny kierunkowe pozwalają osiągnąć znaczny zasięg sieci.
- Brak konieczności podłączania jakichkolwiek kabli podczas przyłączania stacji roboczej do sieci.

Wady sieci bezprzewodowych:

- Jest bardzo droga.
- Jest bardzo wolna.
- Na drodze sygnału nie powinno być żadnych przeszkód.
- Rozwiązania różnych producentów rzadko kiedy są ze sobą kompatybilne

Technologia	Przepustowość bez kompresji	Zasięg [m]	Max liczba węzłów sieci	Zasięg kątowy	Cena [USD]
Area Infra Red	250 kB/s-4 MB/s	4-8	10	120°-130°	1,8-9
HomeRF	2 MB/s	50	>128	dookólny	8-30
Bluetooth	1 MB/s	10	8+248 nieaktywnych	dookólny	5-25
IEEE 802.11	11 MB/s	100	około 10 na każdy punkt dostępu	dookólny	50-150

Bibliografia:

1. „Vademecum Teleinformatyka II”, wyd. IDG Poland S.A Warszawa 2002;
2. „Kompendium wiedzy o sieciach – sieci bezprzewodowe”- dodatek specjalny do miesięcznika Networld nr 9.2002;
3. „Sieci bezprzewodowe od a do g” – artykuł miesięcznika Networld nr 10.2002;
4. www.networld.pl;
5. www.tomshardware.pl;
6. www.enter.pl