R G B WH GR BL Grey Scale #13 C M Y K DANES-PICTA.COM
A 1 2 3 4 5 6 M 8 9 10 11 12 13 14 15 B 17 18 19

12

MINISTERSTWO NAUKI I INFORMATYZACJI
AKADEMIA OBRONY NARODOWEJ

Płk dr hab. inż. Bogdan ZDRODOWSKI
Kpt. dr inż. Jan ZYCH

SIEĆ TECHNOLOGII RADIOWEJ W SYMULATORZE OPERACYJNO-TAKTYCZNYCH DZIAŁAŃ POWIETRZNYCH

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Akademii Obrony Narodowej
Nr 57092

WARSZAWA 2004

Colour Chart #13
Blue Cyan Green Yellow Red Magenta White 3/Color Black
Inches Centimetres
DANES-PICTA.COM

MINISTERSTWO NAUKI I INFORMATYZACJI

AKADEMIA OBRONY NARODOWEJ

BIBLIOTEKA I ARCHIWUM
Nr 57092
Akademii Obrony Narodowej

płk dr hab. inż. Bogdan ZDRODOWSKI

kpt. dr inż. Jan ZYCH

SIEĆ TECHNOLOGII RADIOWEJ W SYMULATORZE OPERACYJNO-TAKTYCZNYCH DZIAŁAŃ POWIETRZNYCH

WARSZAWA 2004

Spis treści

Wyjaśnienie skrótów użytych w opracowaniu

IrDA - ang. Infared Data Association.

MS – Microsoft.

PC – ang. Personal Computer.

SI – system informatyczny.

SO – system operacyjny.

WLAN- ang. Wireless Local Area Network

Wstęp

Opracowanie zawiera wyniki badań możliwości zastosowania sieciowej technologii bezprzewodowej w symulatorze powietrznych działań taktyczno-operacyjnych. Na tle potrzeb, wymagań i ograniczeń, określono niezbędne aspekty technologiczne tego rozwiązania komunikacji symulatora, szczególnie akcentując potrzeby (i możliwości) dostępnego[1] sprzętu technologii bezprzewodowej. W realizacji tego zadania wykorzystaliśmy własne doświadczenia, ale przede wszystkim opieraliśmy się na dostępnej, specjalistycznej literaturze o technologii sieci bezprzewodowych.

Przedmiotem naszych badań były:

- zasady projektowania oraz konstruowania takich sieci, eksponując najistotniejsze elementy ich konstruowania. Praktycznym aspektem proponowanego rozwiązania jest prezentacja konkretnych typów urządzeń i technologii;
- aspekty techniczne stosowanych rozwiązań;
- dostępność finansowa i technologiczna rozwiązań.

Zastosowanie technologii radiowej dla konstruowanego symulatora jest świadomym i przemyślanym rozwiązaniem. Dążąc do zapewnienia w jak największym stopniu nowoczesności konstruowanego symulatora[2] adoptujemy dość awangardowe rozwiązanie, jednocześnie nie przekraczając budżetu przeznaczonego na realizację projektu.

---

[1] W lutym 2004 roku.

[2] Zdrodowski B., Zych J. Symulator operacyjno-taktycznych działań powietrznych - GAMBLER, tom 1, Koncepcja realizacji projektu, AON, Warszawa 2003.

Autorzy spodziewają się, że wprowadzenie sieci bezprzewodowych zapewni:

- pożądaną elastyczność konfigurowania sprzętu stosowanego w symulatorze;
- wystarczającą prędkość transmisji pomiędzy terminalami;
- możliwość rozegrania gry w obrębie nie tylko sali (auli), ale nawet budynku;
- niezawodność na wymaganym poziomie;
- nowoczesność w stosunku do tej klasy systemów użytkowanych w wojsku;
- bezpieczeństwo elementów podsystemu na poziomie akceptowalnym.

Opracowanie mieści się w zadaniu 12[3] harmonogramu przedsięwzięć realizacji projektu.

---

[3] Zdrodowski B., Zych J. Symulator operacyjno-taktycznych działań powietrznych - GAMBLER, tom 1, Koncepcja realizacji projektu, AON, Warszawa 2003.

1. Technologia WLAN

Bezprzewodowa sieć lokalna (ang. WLAN – Wireless Local Area Network) będzie dla symulatora elastycznym systemem komunikacji zaimplementowanym jako uzupełnienie, lub jako rozwiązanie alternatywne dla tradycyjnej sieci kablowej. Najważniejszą cechą takiej sieci z punktu widzenia użyteczności jest to, iż sieć bezprzewodowa łączy w sobie transmisję danych z mobilnością użytkownika. Użytkownicy użytkując taką sieć zyskują na wydajności, używając przenośnych terminali i komputerów do stałej, bieżącej transmisji danych do centralnych systemów przetwarzania. Można zatem postrzegać sieci bezprzewodowe jako doskonałą alternatywną technologię dla wszelkich zastosowań związanych z użytkowaniem symulatora operacyjno-taktycznych działań powietrznych.

Należy podkreślić, że sieci WLAN są szczególnie atrakcyjną alternatywą dla technik przewodowych w sytuacji, gdy z różnych przyczyn instalacja sieci przewodowej jest niemożliwa lub w perspektywie czasu jej instalacja jest nieopłacalna (pokazy na konferencjach, seminariach, ćwiczeniach).

Historia sieci bezprzewodowych sięga II Wojny Światowej. Armia Stanów Zjednoczonych jako pierwsza wykorzystała do transmisji danych sygnał radiowy. Opracowano wtedy technologię transmisji przez radio silnie szyfrowanych danych. Była ona szeroko wykorzystywana w trakcie kampanii prowadzonych przez armie Stanów Zjednoczonych i aliantów. Fakt ten stał się źródłem inspiracji dla grupy pracowników naukowo-badawczych z Uniwersytetu Hawajskiego, która stworzyła pierwszą, radiową sieć

komunikacyjną opartą o transmisję pakietową, znana pod nazwą ALOHNET. W jej skład wchodziło 7 komputerów komunikujących się ze sobą topologii dwukierunkowej gwiazdy pokrywającej cztery hawajskie wyspy. Centralny komputer znajdował się na wyspie Oahu. W ten sposób po raz pierwszy rozpoczęła funkcjonowanie sieć bezprzewodowa.

1.1. Zalety sieci typu WLAN dla potrzeb symulatora

Sieci WLAN[4] charakteryzują następujące zalety[5]:

- **Przenośność** – bezprzewodowe systemy sieciowe umożliwiają użytkownikom sieci dostęp do aktualnych informacji bez względu na lokalizację. Taka przenośność zwiększa wydajność i stwarza możliwość świadczenia usług niedostępnych przy korzystaniu z sieci kablowej.
- **Szybkość i prostota instalacji** – instalacja sieci bezprzewodowej może być szybka i łatwa dzięki wyeliminowaniu potrzeby układania kabli, robienia przepustów przez ściany i kondygnacje.
- **Skalowalność** – bezprzewodowe systemy sieciowe mogą być konfigurowane w różnych topologiach dopasowując je do wymogów danego systemu informatycznego. Łatwo modyfikuje się konfigurację i zasięg sieci, począwszy od indywidualnych użytkowników w układzie peer-to-peer, aż po złożone infrastruktury, które mogą obsługiwać

---

[4] Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.

[5] Vademecum teleinformatyka cz. I, Wyd. IDG Poland S.A., Warszawa 2001.

dużą liczbę użytkowników i/lub znaczny obszar poprzez dodanie kolejnych punktów dostępowych.

Łatwość i prostota obsługi – użytkownicy nie potrzebują zaawansowanej wiedzy, aby korzystać z sieci bezprzewodowej. Cechą sieci bezprzewodowych jest ich „przeźroczystość" dla systemów operacyjnych. Aplikacje pracują tak samo na sieci kablowej.

1.2. Wady sieci typu WLAN dla potrzeb symulatora

Pomimo szeregu zalet, sieci bezprzewodowe posiadają również wady, do których zaliczyć możemy:

- **Koszt szerokości pasma** – mimo znaczącego spadku kosztów ta sama szerokość pasma jest w sieciach bezprzewodowych nadal znacząco droższa niż w sieciach kablowych.
- **Dostępna szerokość pasma** – sieci bezprzewodowe wciąż dysponują dużo mniejszą szerokością pasma niż sieci kablowe.
- **Zasięg** – w wypadku systemów bezprzewodowych jest często poważnie ograniczony, co nie pozwala uzyskać pożądanej funkcjonalności lub wymusza kompromisy.
- **Bezpieczeństwo inwestycji** – obecnie na rynku jest wiele rozwiązań, przy czym tylko niektóre mogą liczyć na sukces w perspektywie średniookresowej.

2. Wybór standardu w sieciach bezprzewodowych

Obserwowany w ostatnich latach dynamiczny rozwój technologii bezprzewodowych doprowadził do wykształcenia w tej dziedzinie kilku standardów. Do najistotniejszych z punktu widzenia zastosowania w lokalnych sieciach komputerowych należą:

- IrDA,
- Bluetooth,
- 802.11,
- HomeRF
- HiperLAN.

Wszystkie wymienione standardy, za wyjątkiem pierwszego, stanowią rozwiązania oparte o technologie radiowe. IrDA została tutaj wymieniona oraz krótko scharakteryzowana w dalszej części opracowania, z uwagi na chęć zaprezentowania pełnego obrazu standardów oraz porównania rozwiązań radiowych z wykorzystującymi transmisje w podczerwieni.

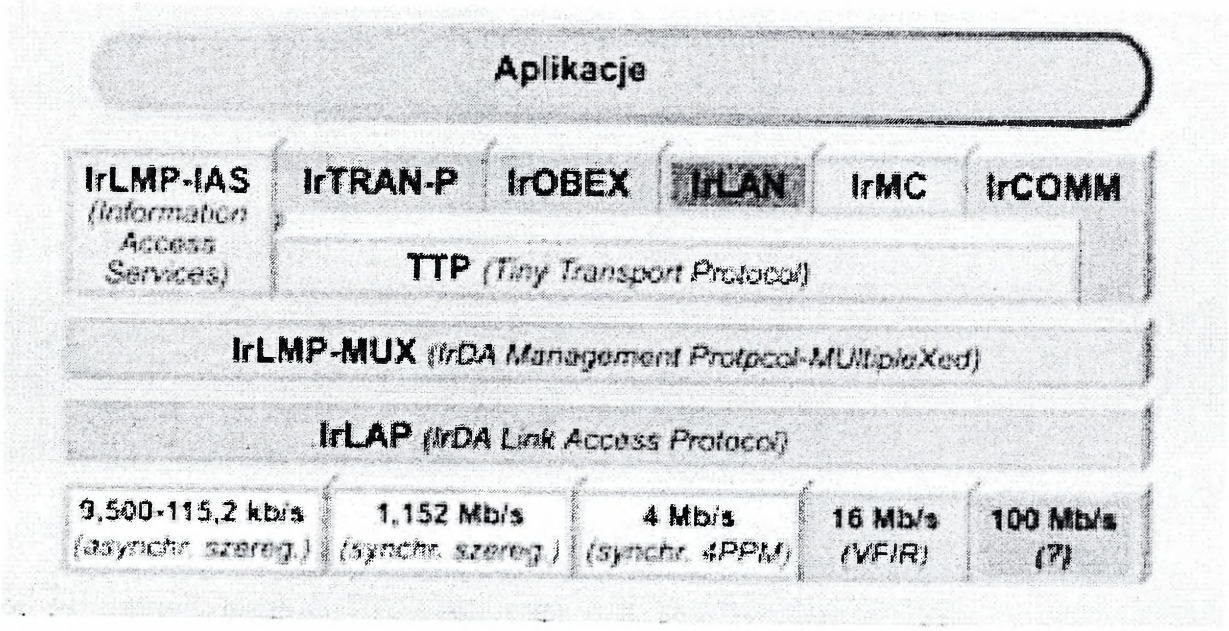
2.1. IrDA (Infared Data Association)

IrDA jest protokołem transmisji cyfrowych w podczerwieni, zawdzięczającym swoje powstanie procesom normalizacyjnym dotyczącym pilotów sterujących odbiornikami TV i magnetowidami. Dzisiaj Forum IrDA specyfikuje trzy standardy komunikacji za pośrednictwem fal podczerwonych:

- IrDA-Data,
- IrDA-Control
- AIr (*Advanced Infrared*).

Obecnie standard 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 30°. Po obniżeniu szybkości transmisji do 75 [kb/s] można komunikować się na odległość ponad 5 [m]. Protokół AIr zapewnia przesyłanie danych w konfiguracji wielopunkt-wielopunkt. Obecnie oferuje przepływność 4 [Mb/s] na odległości 4 [m] lub 250 [kb/s] po podwojeniu tego dystansu.

Protokoły komunikacyjne są w IrDA podzielone na warstwy. Stos protokołów wynika z architektury pokazanej na rysunku 1[6].



Rys. 1. Szkic architektury IrDA

Warstwy w stosie są zwyczajowo podzielone na dwie podgrupy - protokoły implementowane obowiązkowo i protokoły opcjonalne. W skład pierwszej wchodzą:

---

[6] Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.

- **Warstwa fizyczna** (*Physical Layer*), która specyfikuje charakterystyki optyczne, kodowanie danych oraz synchronizowanie ramek.
- **IrLAP** (*Link Access Protocol*), odpowiadająca za niezawodność połączenia.
- **IrLMP** (*Link Management Protocol*) - protokół multipleksowania usług i aplikacji.
- **IAS** (*Intention Access Service*), czyli dostęp do informacji.

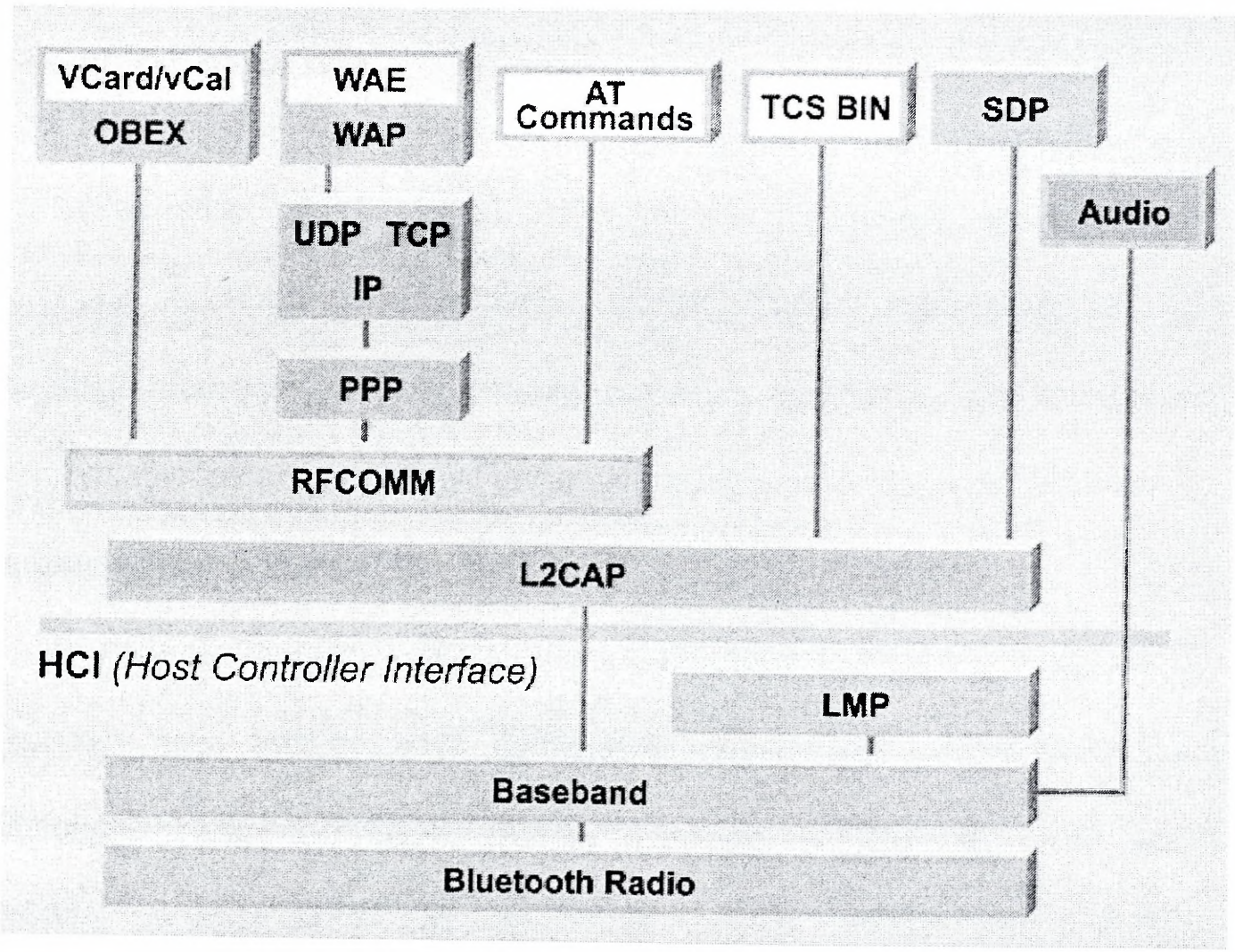
Zastosowanie protokołów opcjonalnych zależy od konkretnej aplikacji. Do grupy tej należą:

- **TinyTP** (*Tiny Transport Protocol*), zapewniający sterowanie strumieniem w kanale. Jest to bardzo ważna funkcja i z tej racji często rekomendowana dla wielu aplikacji.
- **IrOBEX** (*Object Exchange Protocol*), ułatwiający transfer plików oraz innych obiektów danych.
- **IrCOMM**, którego głównym zadaniem jest emulowanie portów szeregowego i równoległego, opartych na 4 typach usług: 3-Wire Raw, 3-Wire, 9-Wire i Centronics.
- **IrLAN** (*Local Area Network*), zapewniający dostęp urządzeniom, np. notebookom, do sieci lokalnej za pośrednictwem podczerwieni.

2.2. Bluetooth

Bluetooth jest to otwarty standard bezprzewodowej komunikacji, promowany głównie przez firmy zajmujące się produkcją komputerów osobistych i

telefonów komórkowych. Zgodnie z założeniami ma on usprawnić komunikację między urządzeniami peryferyjnymi, a komputerami osobistymi. Bluetooth jest bardzo podobny do protokołu IrDA, z tą różnicą, że stosuje częstotliwości radiowe. Niemniej jego pasmo przenoszenia 2,5 [GHz] ISM (*Industrial Scientific Medical*) nie było jeszcze licencjonowane. W przyszłości jego zakres aplikacyjny zostanie poszerzony o komunikację z systemami, takimi jak np. sterowania ogrzewaniem.



Rys. 2. Architektura standardu Bluetooth[7]

Bluetooth powstał w 1994 r. w Szwecji. Nazwa tego protokołu to przydomek żyjącego w X w. duńskiego króla Haralda I - "Blaatand" (czyli

[7] Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.

"Sinozęby") to po angielsku właśnie "Bluetooth". W 1998 r. utworzono SIG (*Special Interest Group*) - grupę, w skład której weszły tak poważne przedsiębiorstwa jak: Ericsson, IBM, Intel, Nokia i Toshiba. Z czasem dołączyły do niej następne - 3Com, Microsoft, Lucent Technologies czy Motorola. Teraz jest ich ponad 2000.

Bluetooth próbuje zyskać przewagę nad innymi technologiami przesyłania danych na krótkich dystansach, jak IrDA czy HomeRF, które są przeznaczone na podobny rynek. Mimo deklaracji SIG o komplementarności z IrDA staje się powoli jasne, że obydwie technologie są konkurencyjne dla komunikacji między PC a urządzeniami peryferyjnymi. IrDA zdobyła już pewną popularność w środowisku urządzeń peryferyjnych. Jednak trudno zaprzeczyć, że ta technologia transmisji w podczerwieni ma kilka ograniczeń, do których w pierwszym rzędzie trzeba zaliczyć niewielki zasięg oraz konieczność ustawiania urządzeń w "polu widzenia" PC.

Bez anteny kierunkowej zasięg jest ograniczony do ok. 10 metrów, ale w przyszłości mają być dostępne dodatkowe wzmacniacze, w których moc wyjściowa wzrośnie z 1 do 100 [MW], a zasięg zwiększy się do ok. 100 metrów.

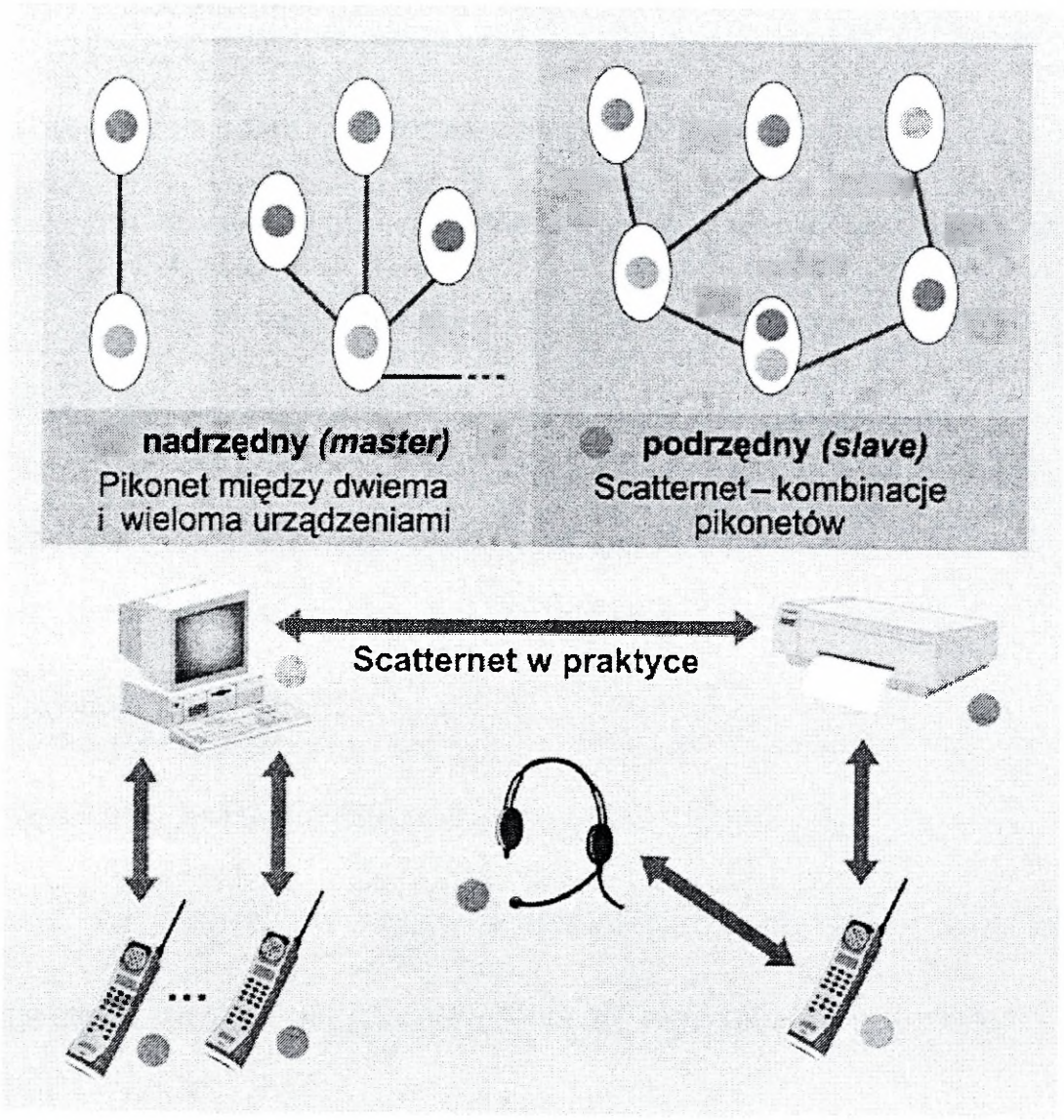
Bluetooth obsługuje zarówno synchroniczny jak i asynchroniczny typ transmisji. Dzięki temu umożliwia przesyłanie mowy w paśmie o szerokości 64 [kb/s] w obu kierunkach oraz przesyłanie danych w paśmie o szerokości 865,2 [kb/s].

Standard definiuje nie tylko niższe poziomy warstwy protokołów, lecz również usługi opisane na wyższych poziomach. Dzięki temu w komfortowy sposób obsługuje tworzenie tzw. sieci ad hoc (por. rys. 7).

Obszar zastosowań Bluetooth, ze względu na wymienione cechy kluczowe, to zdecydowanie sieci osobiste. Tworzenie wydajnych sieci lokalnych nie jest możliwe ze względu na niską przepustowość i ograniczenia technologii.

Główną siłą Bluetooth jest zdolność do równoczesnej transmisji danych i dźwięku. Możliwa jest asynchroniczna transmisja danych w jednym kanale i do trzech transmisji synchronicznych dźwięku w trzech kanałach. Dane i dźwięk można też przesłać jednym kanałem.

Urządzenia Bluetooth są zorganizowane w grupy (podsieci), liczące od dwu do ośmiu urządzeń, zwane pikonetami (*piconets*), składające się z jednego urządzenia nadrzędnego (*master*) i jednego lub kilku urządzeń podrzędnych (*slave*). Urządzenie może należeć do więcej niż jednej podsieci, przy czym urządzenie podrzędne pozostaje takim w każdej z nich - spełnia ono rolę mostu łączącego kilka podsieci w sieć rozproszoną (*scatternet*). (rys.3) zaprezentowano taką konfigurację.



Rys.3[8]. Podsieci i siec rozproszona w Bluetooth.

Jak wspomniano, Bluetooth funkcjonuje w nielicencjonowanym paśmie ISM, wykorzystywanym przez wiele urządzeń, w tym kuchenki mikrofalowe. Dla wzmocnienia urządzeń zgodnych z tym standardem, każdy pikonet jest zsynchronizowany ze specjalnym wzorcem skoku częstotliwościowego. Wzorzec ten, przemieszczający się w jednej sekundzie 1600 razy, jest unikatowy dla danego pikonetu. Każdy przeskok na określoną częstotliwość jest w istocie szczeliną czasową, w której transmituje się dane. Pakiet może obejmować do pięciu szczelin czasowych. W takich przypadkach skok do innej

[8] Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.

częstotliwości następuje po ostatniej szczelinie. W protokole Bluetooth określono rozszerzanie widma przez pseudolosowe skakanie po 79 częstotliwościach w paśmie rozproszonym 2,402-2,480 [GHz]. Liczba skoków w ciągu sekundy wynosi 1600. Różnica między częstotliwościami po skokach jest całkowitą krotnością 1 [MHz]. Dla większości krajów Europy i w USA częstotliwości skoków wynoszą f = 2,402 [GHz] + k [MHz], gdzie k = 0, 1, 2, ... 78. W niektórych krajach stosuje się tymczasowo system 23 skoków - w Hiszpanii f = 2,449 + k [MHz], a k = 0, 1, ... 22. We Francji f = 2,454 + k [MHz], gdzie k = 0, 1, ... 33.

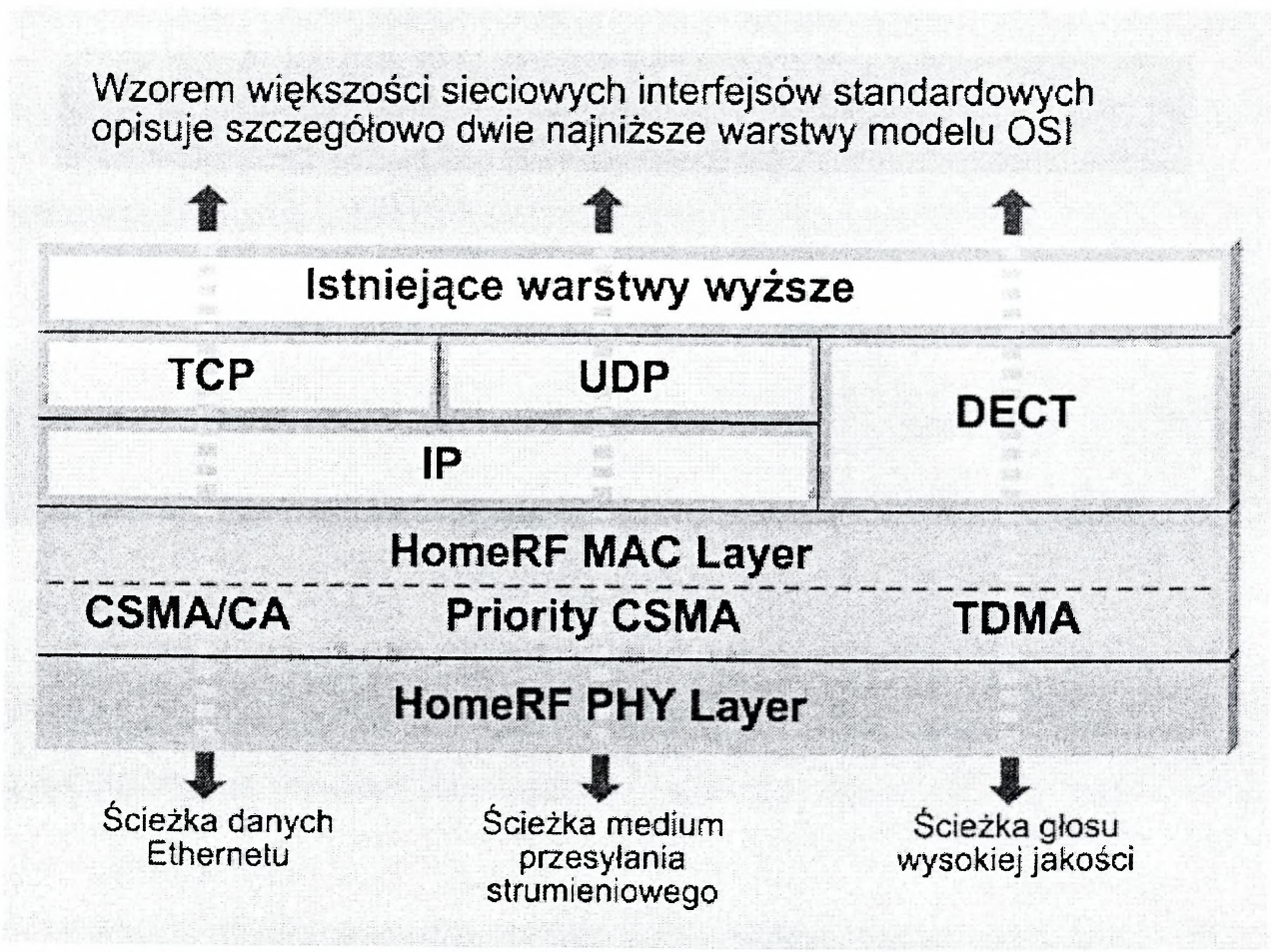
Pikonety mogą być formowane zarówno statycznie, jak i dynamicznie, kiedy urządzenie wejdzie w zasięg drugiego lub kiedy go opuści. Jeśli adres punktu przeznaczenia jest nieznany, używa się zapytań. Po odpowiedzi zdalnego urządzenia obydwa urządzenia wchodzą w opisany wcześniej stan połączenia, przy czym urządzenie inicjujące staje się nadrzędnym, a odpowiadające podrzędnym.

W stanie połączenia urządzenie podrzędne będzie synchronizowane z zegarem urządzenia nadrzędnego i z prawidłowym wzorcem skoku częstotliwości. W takiej chwili układy zarządzające łączem wymieniają odpowiednie polecenia, żeby ustalić łącze. Urządzenie nadrzędne będzie wtedy inicjowało regularnie transmisję, utrzymującą zsynchronizowanie pikonetów. Z kolei urządzenia podrzędne, przez nasłuch każdej szczeliny czasowej transmitowanej przez urządzenie nadrzędne, mogą się z nim zsynchronizować.

Technologia Bluetooth nie przybrała jeszcze swojego ostatecznego kształtu. Grupa SIG ciągle pracuje nad zwiększeniem przepływności, poprawą bezpieczeństwa czy odporności na zakłócenia.

2.3. HomeRF

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. Niedawno powstała wersja 2.0 tego standardu. Jak większość specyfikacji dotyczących standardów interfejsów sieciowych opisuje dokładnie dwie najniższe warstwy modelu OSI.



Rys. 4[9]. Specyfikacja standardu HomeRF.

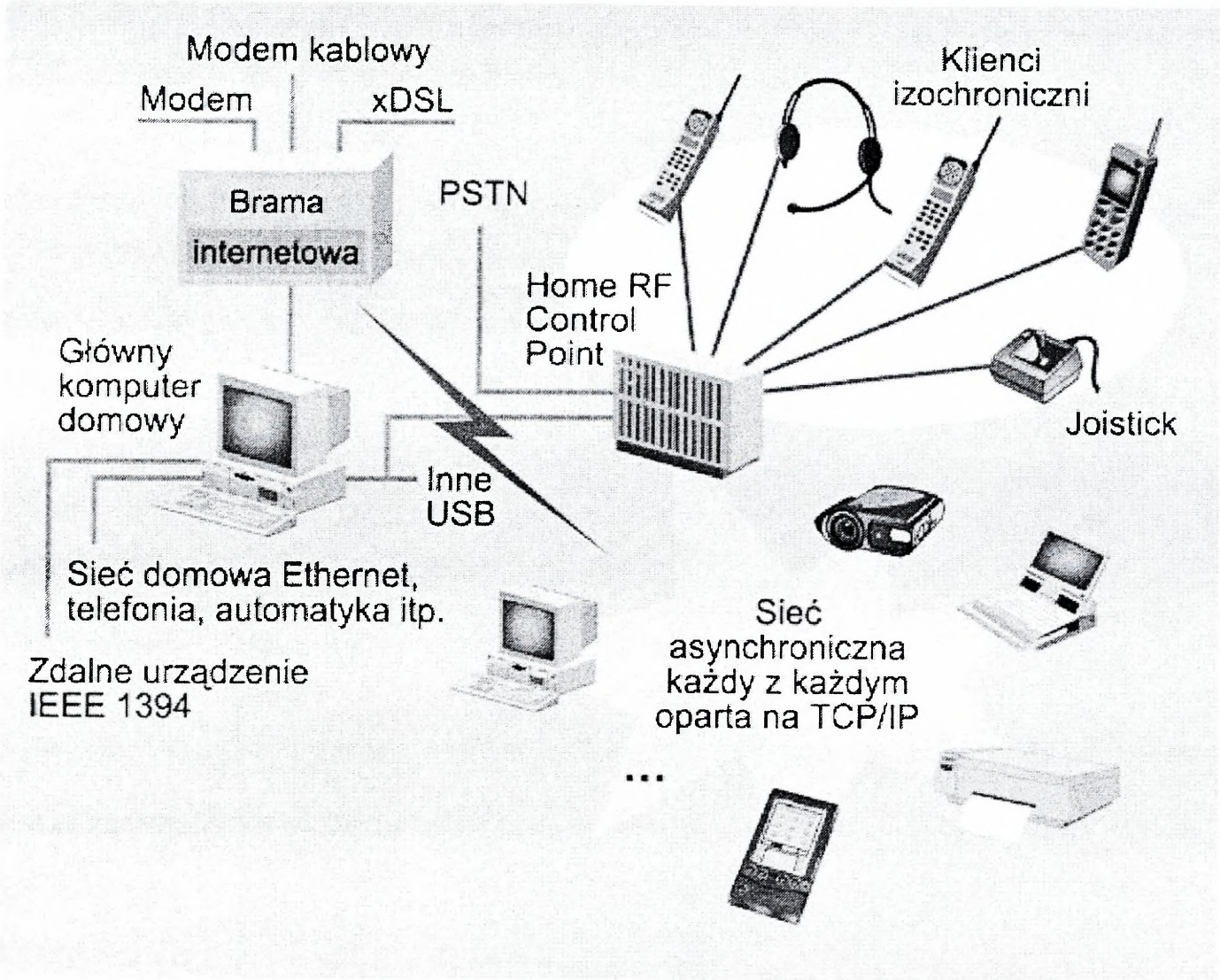
[9] Op. Cit.

Warstwa fizyczna ustala szybkość przesyłania danych i zakres charakterystyk. Warstwa wyższa (łącza danych) - tutaj używana podwarstwa MAC (*Media Access Control*) - definiuje typy obsługi danych (jak wideo), ale także inne atrybuty, takie jak: bezpieczeństwo, *roaming* i odwzorowanie adresów (mapowanie).

Standard HomeRF (RF – radio frequency) próbuje przezwyciężyć słabości standardu IEEE802.11. Równolegle z danymi można w nim przesyłać mowę względnie pakiety multimedialne. Pierwsza wprowadzona na rynek wersja standardu 1.2 obsługiwała transfer do 1,6 [Mb/s]. Kolejne 2,0 i 2,1 obsługują odpowiednio do 10 [Mb/s] i do 20 [Mb/s].

HomeRF pracuje w nielicencjonowanym paśmie 2,4 [GHz]. Korzysta z techniki skokowej zmiany częstotliwości. Wyróżnionych jest 75 kanałów o szerokości pasma 1 MHz, każdym z nich można przesłać 1,6 Mb/s. W nowszych wersjach uzyskuje się wyższy transfer dzięki łączeniu kanałów. Zasięg systemów HomeRF wynosi 50 metrów. Oprócz transmisji danych HomeRF umożliwia przesyłanie głosu i multimediów o określonych parametrach jakościowych.

Opis standardu HomeRF obejmuje dwie niższe warstwy sieci. Są wyposażone w punkty dostępu do usługi w taki sposób, że mogą każdorazowo prawidłowo obsłużyć różne rodzaje ruchu (dane, multimedia, głos). (por. rys. 5)



Rys. 5[10]. Wizja rozwoju HomeRF

Zaletą systemu jest ekonomiczna realizacja zarówno przesyłu danych, jak i telefonii. Nie był projektowany do poważnych zastosowań biurowych i się do nich nie nadaje. Jeśli staniejąwydajniejsze systemy 802.11, HomeRF gwałtownie straci na atrakcyjności.

2.4. HiperLAN

W standardzie HiperLAN Type 2 za cel postawiono zapewnienie dostępu do stałej sieci z prędkością do 155 [Mb/s] zarówno w warunkach domowych, jak i biurowych. HiperLAN/2 pracuje w paśmie 5 [MHz]. Wykorzystuje technikę OFDM (orthogonal frequency division multiplex), podobnie jak ADSL. OFDM uzyskuje wysoką wydajność również w kanałach rozproszonych, jakie

[10] Op. Cit.

występują w zakresie częstotliwości gigahercowych. Oprócz tego stosuje się modulację typu Multicarrier Modulation. W tej technice dane przesyłane są na niezależnych podnośnych. Każdy kanał dysponuje 48 podnośnymi dla danych i 4 podnośnymi pilotowymi do synchronizacji.

HiperLAN/2 uzyskuje na poziomie fizycznej warstwy transportowej przepustowość 54 [Mb/s]. Jako bezprzewodowy wariant ATM uzyskuje podobną do niego jakość usług.

Specyfikacja HiperLAN/2 ogranicza się do opisu obu dolnych warstw sieci. Typowa sieć HiperLAN/2 składa się z wielu punktów dostępowych (access point AP), które łącznie zapewniają dostęp na pewnym obszarze. W tak utworzonych komórkach odbywa się komunikacja mobilnych użytkowników (mobile terminals MT). Możliwy jest tryb centralized mode (CM), w którym wszyscy użytkownicy mobilni przesyłają dane przez punkty dostępowe, lub tryb direct mode (DM), w którym użytkownicy mobilni, którzy znajdują się we wzajemnym zasięgu, wymieniają dane bezpośrednio pod nadrorem instancji nadzorującej (central controller CC)

HiperLAN/2, podobnie jak kablowa sieć ATM, zorientowany jest na połączenia. Przed rozpoczęciem transmisji danych użytecznych konieczne jest nawiązanie połączenia; wariantowo może być to połączenia punkt-punkt, punkt-wiele punktów lub połączenie rozgłoszeniowe.

2.5. WLAN 802.11b

Sekcja standaryzacyjna amerykańskiego stowarzyszenia inżynierów IEEE opracowała protokół transmisji bezprzewodowej IEEE802.11, podobny do

wszechobecnego Ethernetu. Z kolei Wireless Ethernet Compatibility Alliance (WECA) certyfikuje urządzenia kompatybilne z 802.11 pod względem wzajemnego współdziałania. Dlatego też urządzenia pracujące w standardzie 802.11 sprzedawane są również pod nazwą handlową Wi-Fi (Wireless Fidelity).

Oprócz pierwotnego standardu są trzy ważne rozszerzenia. 802.11b i 802.11g umożliwiają przechodzenie – z uwzględnieniem stosowanych systemów 802.11 – na szybszą transmisję. 802.11a jest standardem podobnym, jednak niekompatybilnym ze względu na inną częstotliwość nośną.

Norma 802.11b została zatwierdzona przez IEEE we wrześniu 1999. Zapewnia ona transmisje do 11 Mb/s w pasmie 2,4 [MHz]. Podobnie jak w innych systemach bezprzewodowych autorzy zdefiniowali tylko dwie najniższe warstwy odpowiadające OSI: fizyczną i łącza wraz z podwarstwą MAC.

Rys. 6. Standard IEE 802.11b na tle modelu OSI

W normie tej zdefiniowano również dwa podstawowe składniki:

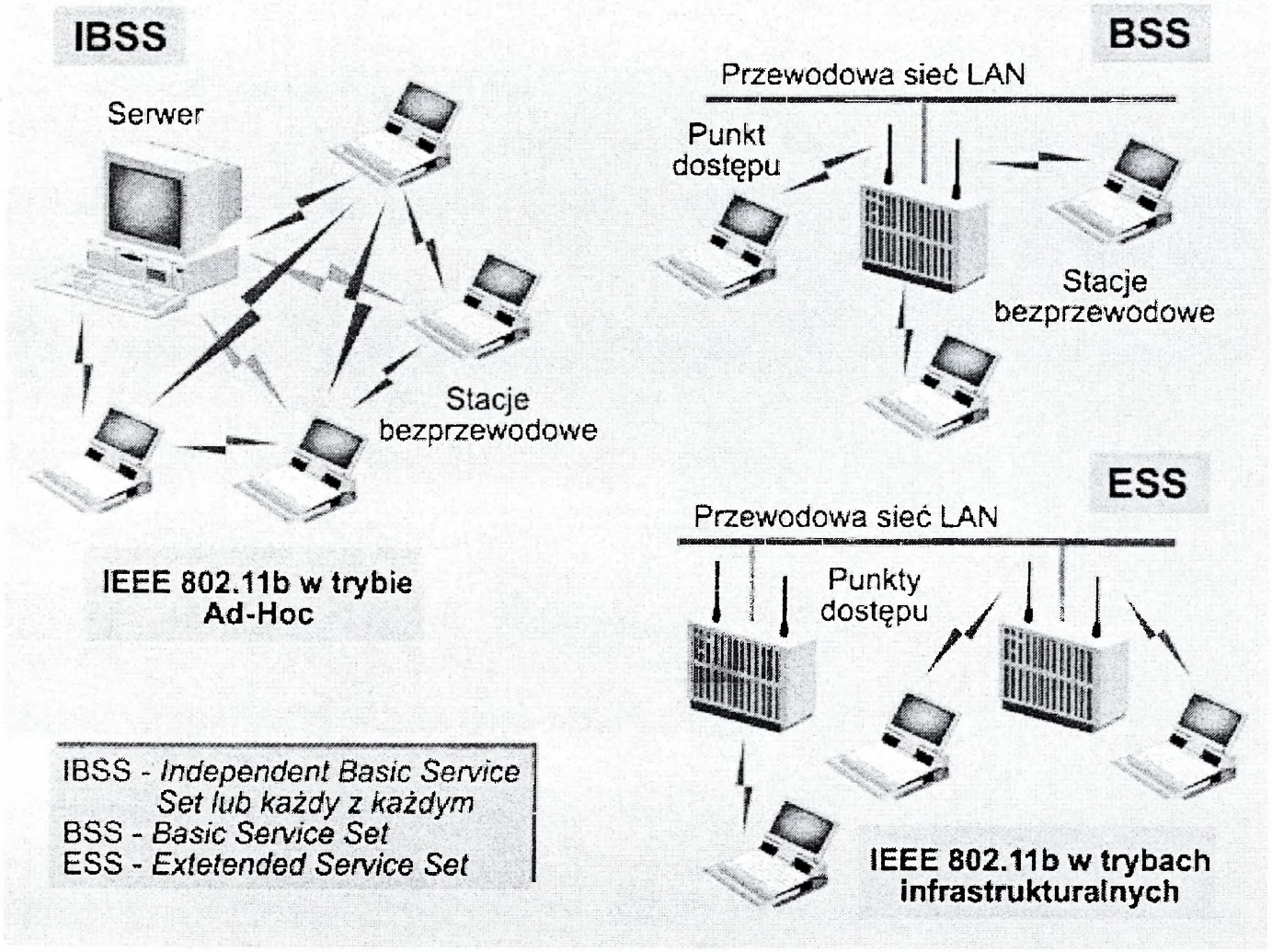
- komputer osobisty lub notebook wraz z kartą sieciową;

- punkt dostępu - AP (*Access Point*), który funkcjonuje jak most między bezprzewodowymi stacjami lub między stacjami, a systemem dystrybucyjnym, czyli siecią przewodową.

802.11b funkcjonuje w dwu trybach: **infrastrukturalnym** i **ad hoc** (rys. 7).

W sieciach ad hoc, iż wraz ze wzrostem odległości między punktami sieci maleje transfer danych, gdyż większość modeli kart sieciowych (zwłaszcza PCMCIA) jest wyposażona w zbyt słabe nadajniki i anteny. Zdarza się, że utrzymanie nieprzerwanego połączenia pomiędzy komputerami znajdującymi się nawet w sąsiednich pokojach jest niemożliwe. Inną trudnością, jest pojemność sieci ad hoc. W zależności od rodzaju użytych kart sieciowych może się ona składać ze 156 lub 256 stacji roboczych, choć w praktyce nie powinno ich być więcej niż 25-30.

Wszędzie tam, gdzie niemożliwe jest zastosowanie sieci ad hoc, wykorzystuje się stację bazową nazywaną punktem dostępowym (ang. access point). Punkt dostępowy stanowi rodzaj pośrednika przekazującego informacje z jednego komputera do drugiego. Co ważne, punkt dostępowy ma lepsze parametry techniczne (m.in. zapewnia większy zasięg) niż karta sieciowa, ponieważ wyposażony jest w anteny nadawczo-odbiorcze większej mocy. Łączność bezprzewodowa za pośrednictwem punktu dostępowego jest najczęściej wykorzystywanym trybem komunikacji.



Rys. 7[11]. Podstawowe konfiguracje pracy sieci 802.11b

Warstwa ta obejmuje fizyczny interfejs między urządzeniami i zajmuje się transmitowaniem bitów w kanałach komunikacyjnych. W technologii 802.11b zaimplementowano system umożliwiający dynamiczne dostosowanie się do poziomu zakłóceń. W zależności od tego poziomu osiągana przepływność może wynieść 11, 5,5, 2 i 1 [Mb/s]. Systemy 802.11 mogą stosować modulację DSSS (*Direct Sequence Spread Spectrum*) i FHSS (*Frequency Hopping Spread Spectrum*). W USA nie można stosować modulacji FHSS dla przepływności przekraczających 2 [Mb/s] z uwagi na regulacje komisji federalnej - FCC (*Federal Communications Commission*). Może dlatego większość systemów 802.11b wykorzystuje modulację DSSS?

[11] Op. Cit.

Warstwa fizyczna dzieli się na dwie podwarstwy: PLCP (*Physical Layer Convergence Protocol*) i PMD (*Physical Medium Dependent*). PMD jest odpowiedzialna za kodowanie, PLCP daje wspólny interfejs dla sterowników wyższych warstw.

Podwarstwa MAC służy jako interfejs między warstwą fizyczną a komputerem. Obsługuje obydwa wcześniej wymienione tryby. Dwiema najważniejszymi funkcjami tej podwarstwy są: cykliczna kontrola nadmiarowości CRC (*Cyclic Redundancy Check*) i fragmentacja pakietów. Dzięki tej drugiej funkcji duże pakiety mogą być wysyłane w mniejszych fragmentach. Ma to dwie zalety. Pierwsza polega na zredukowaniu retransmisji pakietów - prawdopodobieństwo uszkodzenia pakietu wzrasta wraz ze wzrostem jego długości. Druga korzyść: w razie błędu węzeł musi dokonać retransmisji tylko niewielkiego fragmentu całości, co jest dużo szybsze.

2.6. Rekomendacje IEEE 802.11

Standard 802.11 został przyjęty w roku 1997 jako oficjalny standard bezprzewodowego interfejsu, stanowiąc odmianę klasycznego Ethernetu (802.3) – (tabela 1).

Tabela 1. Najważniejsze standardy rodziny IEEE 802

<table>
<tr><td rowspan="4">802.10 bezpieczeństwo</td><td rowspan="4">802.2 przegląd i architektura</td><td rowspan="4">802.1 Management</td><td colspan="6">802.2 Logical Link Control</td><td rowspan="2">Warstwa łącza danych</td></tr>
<tr><td colspan="6">802.1 Bridging</td></tr>
<tr><td>802.1 MAC</td><td>802.5 MAC</td><td>802.6 MAC</td><td>802.11 MAC</td><td>802.15 MAC</td><td>802.16 MAC</td><td rowspan="3">Warstwa fizyczna</td></tr>
<tr><td>802.1 PHY</td><td>802.5 PHY</td><td>802.6 PHY</td><td>802.11 PHY</td><td>802.15 PHY</td><td>802.16 PHY</td></tr>
<tr><td>Ethernet</td><td>Token Ring</td><td>DQDB</td><td>WLAN</td><td>WPAN</td><td>WMAN</td></tr>
</table>

Rodzina rekomendacji IEEE 802.11, dotycząca sieci bezprzewodowych, przedstawia się następująco:

- **802.11** - oficjalna rekomendacja IEEE z 1997 r., norma sieci bezprzewodowej o przepływności 1 lub 2 Mb/s w pasmie 2,4 GHz, przy użyciu jednej z dwu metod modulacji - FHSS lub DSSS;
- **802.11a** - rozszerzenia do 802.11. Bezprzewodowa sieć lokalna osiąga przepływność 54 Mb/s w pasmie radiowym 5,8 [GHz]. Schemat kodowania - OFDM. Norma ta nie jest akceptowana w Europie, gdyż pasmo 5 [GHz] zarezerwowano dla HiperLAN;
- **802.11b** - rozszerzenia do 802.1, znane także pod nazwami 802.11 *High Rate* lub *Wi-Fi*. Szybkość transmisji w bezprzewodowej sieci lokalnej wynosi 11 Mb/s w pasmie radiowym 2,4 [GHz]. Modulacja - tylko DSSS;

802.11d - wymagania i parametry niezbędne do aplikowania 802.11 na różnych kontynentach;

- **802.11e** - zarządzanie jakością usług QoS w sieciach 802.11a, b oraz g;
- **802.11f** - współdziałanie w jednej sieci punktów dostępu pochodzących od różnych producentów. Jednym ze składników 802.11f jest IAPP (*Inter-Access Point Protocol*) - roaming między komórkami 802.11;
- **802.11g** - standard warstwy fizycznej sieci WLAN w pasmach 2,4 i 5 [GHz], wspierający modulacje OFDM i CCK. Specyfikuje trzy kanały radiowe. Maks. szybkość - 54 [Mb/s] na kanał;
- **802.11h** - uzupełnienie MAC odnoszące się do europejskich regulacji dla sieci WLAN w pasmie 5 [GHz] (kontrola mocy TCP i dynamiczny przydział kanałów radiowych - DFS);
- **802.11i** - metodyka bezpieczeństwa i uwierzytelnienia użytkowników sieci 802.11a, b oraz g. Ważnymi składnikami 802.11i jest protokół TKIP (*Temporal Key Integrity Protocol*) i szyfrowanie AES (*Advanced Encryption Standard*);
- **802.11j** - zarys przyszłościowej normy globalnej zgodnej z IEEE 802.11 i ETSI HiperLAN2;
- **802.1X** - struktura uwierzytelnienia. Protokoły EAP-TLS, LEAP lub EAP-TTLS. Uwierzytelnianie za pośrednictwem serwera obsługującego EAP, metodyka dynamicznej dystrybucji kluczy itp.

3. Problemy wynikające z zastosowania sieci bezprzewodowych dla symulatora

Sieci bezprzewodowe są same w sobie pewnym czynnikiem ryzyka. Fale radiowe nie rozchodzą się tylko w wąsko pojętym obrębie sieci. Dane można odebrać za pomocą dowolnego odbiornika IEEE802.11, znajdującego się w zasięgu. Dlatego też w standardzie zaimplementowano wiele mechanizmów bezpieczeństwa.

Na najniższym poziomie uczestnicy uzyskują dostęp za pomocą klucza electronic system ID (SSID, ESSID). Klucz SSID, identyczny dla wszystkich systemów w sieci, ustala administrator podczas konfiguracji klientów i punktów dostępowych. Wynikają stąd dwa ograniczenia, znajomość SSID wskazuje, że użytkownik dysponuje ogólnymi prawami dostępu, jednak nie wynika z tego żadna możliwość zidentyfikowania go. Ponadto ustalenie SSID sieci WLAN często nie stanowi żadnego problemu.

W sieciach infrastrukturalnych można ograniczyć dostęp poprzez określenie uprawnionych stacji. Stacje biorące udział w komunikacji mogą wymieniać informacje o swojej tożsamości w ramach tzw. **link layer authentications**. Aby było to możliwe, administrator musi wpisać adresy MAC urządzeń na listy dostępu w punktach dostępowych.

Aby umożliwić uwierzytelnianie nie tylko na poziomie urządzeń, lecz również w odniesieniu do użytkowników, większość producentów implementuje od jakiegoś czasu Remote Authentication Dial-in User Service (RADIUS). Umożliwia on centralne zarządzanie użytkownikami.

Treść informacji przesyłanych drogą radiową można szyfrować za pomocą Wired Equvalent Privacy (WEP), wykorzystującego 40-bitowy algorytm RC4. Jest to jednak opcjonalny składnik standardu, który niekoniecznie musi wchodzić w skład każdej implementacji. W przypadku WEP mamy do czynienia ze stosunkowo łatwym do złamania szyfrem o sile zaledwie 40 bitów, co stało się przyczyną wielu dyskusji na temat bezpieczeństwa sieci WLAN. Większość producentów oferuje oprócz szyfrowania 40-bitowego również szyfrowanie 128-bitowe. Ponieważ mechanizmy zabezpieczające wyższych poziomów protokołu, jak choćby IPSec, są wpisane w standard IEEE 802, można je również bez problemu stosować w sieci WLAN.

Aktualnie prace nad rozwijaniem bezpieczeństwa sieci bezprzewodowych idą w kierunku modelu scentralizowanego, łatwego w zarządzaniu. W tym celu opracowuje się pewne rozszerzenia WEP-a. Prace nad nimi, nie zostały jeszcze zakończone, lecz czołowi producenci (np. Cisco, 3Com) już proponują odpowiednie rozwiązania oparte na WEP oraz oferowanym przez IETF protokole Extensible Authentication Protocol (EAP). W założeniach mają one pozwolić na:

- obustronne uwierzytelnianie (klient – siec oraz sieć – klient)
- dynamiczne dostarczanie kluczy szyfrujących po uwierzytelnieniu
- scentralizowane zarządzanie sesjami.

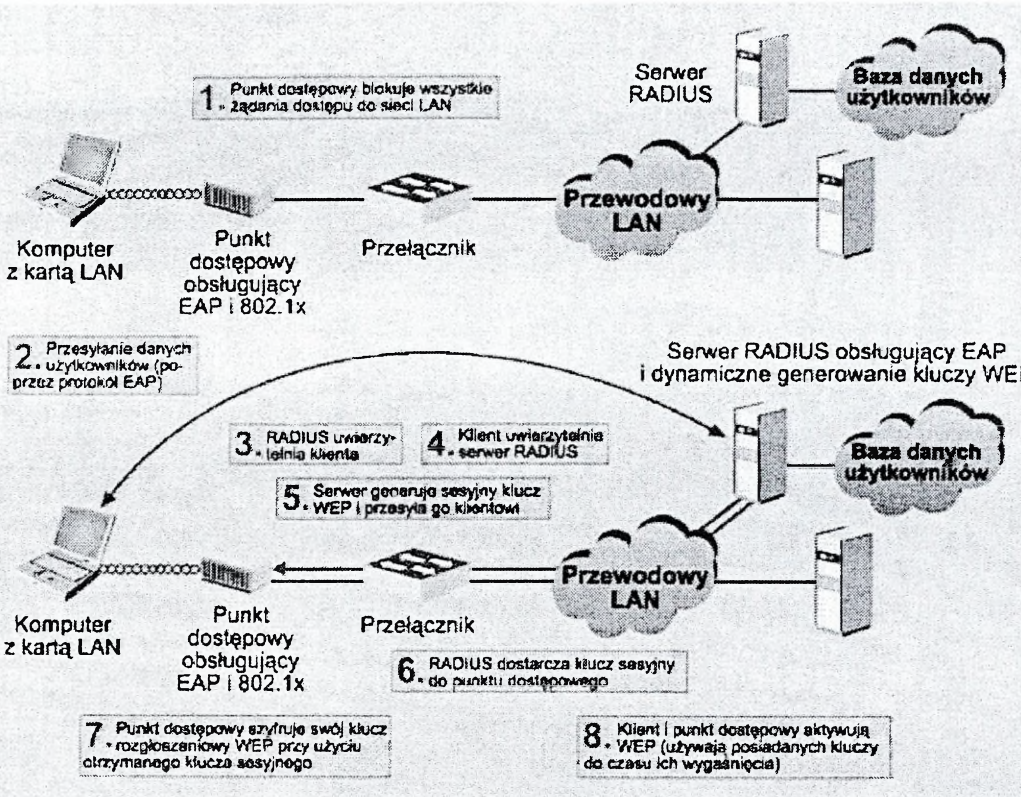
Bezpieczeństwo sieci WLAN zapewniane bywa często przez rozwiązania zaczerpnięte z świata sieci przewodowych. Przykładem takiego rozwiązania jest

zastosowanie serwera RADIUS (rys. 8). Dzięki temu otrzymujemy znaczący wzrost bezpieczeństwa, gdyż:

- wzajemne uwierzytelnienie zapobiega atakom polegającym na podstawieniu fałszywego punktu dostępowego i przechwyceniu haseł użytkownika,
- scentralizowane zarządzanie i dystrybucja kluczy sprawiają, że w przypadku kradzieży nie jest wymagana rekonfiguracja każdego urządzenia,
- możemy zdefiniować częstość zmiany kluczy szyfrujących.

Protokołu EAP dostępny jest w kilku wariantach, różniących się sposobem uwierzytelniania użytkownika. Do najczęściej spotykanych należą (tabela 2):

- EAP-Cisco Wireless (LEAP),
- EAP-Transport Laser Security (EAP-TLS) - (opracowany przez IETF - RFC2716)
- EAP-Tunneled TLS (EAP-TTLS) - (opracowany przez IETF - RFC2716)
- Protected EAP, - (opracowany przez Microsoft, Cisco Systems oraz RSA Security)
- EAP-Subscriber Identity Module (EAP-SIM) – oparty na rozwiązaniach znanych z GSM.



Punkt dostępowy blokuje dostęp do sieci bezprzewodowemu klientowi do momentu pomyślnego zakończenia logowania.
Klient wysyła swoje dane (identyfikator, hasło lub cyfrowy podpis) poprzez EAP.
Używając EAP, serwer RADIUS przeprowadza wzajemne uwierzytelnienie w dwóch fazach. Najpierw weryfikuje dane nadesłane przez klienta i później wysyła mu swoje. Klient weryfikuje serwer RADIUS, kończąc tym samym uwierzytelnienie.
Po pozytywnym zakończeniu klient otrzymuje od serwera klucz WEP, który zostanie użyty w czasie logowania.
Serwer RADIUS za pośrednictwem przewodowej sieci wysyła klucz WEP, nazywany sesyjnym, do punktu dostępowego.
Punkt dostępowy szyfruje swój klucz otrzymanym kluczem sesyjnym i wysyła do klienta, który go deszyfruje za pomocą posiadanego klucza.
Klient oraz punkt dostępowy uaktywniają WEP i używają kluczy: rozgłoszeniowego i sesyjnego do czasu ich wygaśnięcia i wygenerowania kolejnej pary.
Obydwa klucze zmieniają się w regularnych odstępach czasu, który jest definiowany na koniec uwierzytelnienia z użyciem protokołu EAP. Niezależnie od tego częstość zmian klucza rozgłoszeniowego może zostać skonfigurowana w punkcie dostępowym.

Rys. 8. Przebieg uwierzytelniania za pomocą protokołu EAP

Tabela. 2 Porównanie rozwiązań zwiększających bezpieczeństwo sieci WLAN.

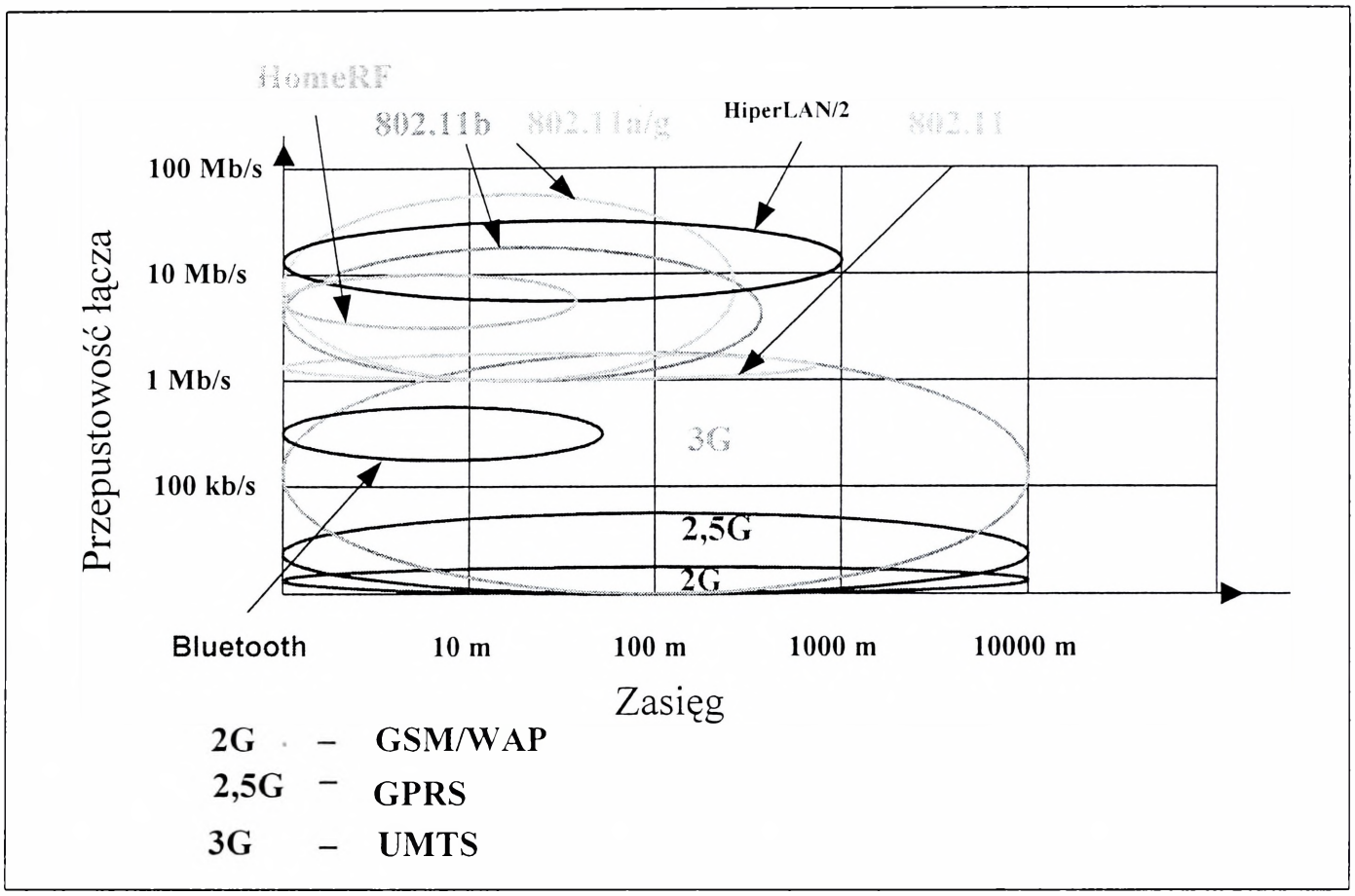
	Cisco LEAP	**EAP-TLS**	**EAP-PEAP**	**EAP-SIM**	**Ipsec**
Długość klucza użytego do szyfrowania [bity]	128	128	128	128	128,192,256
Algorytmy szyfrujące	RC4	RC4	RC4	A3, A8, RC4	3DES lub AES
Identyfikacja urządzenia	Nie	Certyfikat cyfrowy	Nie	Zgodna ze standardem GSM	Certyfikat cyfrowy
Identyfikacja użytkownika	Login, hasło	Certyfikat cyfrowy	Login, hasło, dostęp jednorazowy, certyfikat cyfrowy	Oparta na karcie SIM	Login, hasło, dostęp jednorazowy,
Możliwość stworzenia listy zaufanych użytkowników	Opcjonalna	Opcjonalna	Opcjonalna	Nie	Wymagana
Wymagane rozszerzenie sprzętowe w stosunku do EAP	Nie	Serwer certyfikatów	Serwer certyfikatów	Most z siecią GSM	Koncentrator Ipsec

Na podkreślenie zasługuje również fakt, iż w dziedzinie sieci bezprzewodowych również konstruowane są systemy IDS. Przykładem może być bezprzewodowy IDS (Itrusion Detection System) opracowany przez IBM. Wykorzystując technikę sniffing-u, pozwala wykrywać obecność nieautoryzowanych punktów dostępu, ataki DoS, niepoprawnie skonfigurowane punkty dostępu i narażone klucze szyfrujące WEP. Usługa opiera się na sieci urządzeń linuksowych, które działają jako bezprzewodowe sensory i wdrażane są w sposób podobny do bezprzewodowych punktów dostępu w biurach.

Sensory te monitorują działanie sieci, używając opracowanych przez IBM sygnatur ataków bezprzewodowych. Ostrzeżenia o możliwych atakach są przekazywane do konsoli Tivoli Risk Manager w centrum operacyjnym IBM Global Service. Centrum to, działające całą dobę, umożliwia szybką reakcję na atak. Rozwiązanie jest podobne w działaniu do tradycyjnych IDS, ale inna jest reakcja - w tym przypadku napastnik jest zazwyczaj "w zasięgu ręki", w sieciach tradycyjnych może być oddalony o tysiące kilometrów. IBM nie jest jedynym dostawcą tego typu rozwiązania. Np. firma AirDefence sprzedaje IDS także oparty na sieci rozproszonych sensorów monitorujących bezprzewodowe punkty dostępu. Najnowsze wydanie tego produktu, oprócz wykrywania nielegalnych działań, pozwala również na zdalne wyłączenie takiego punktu. Obsługuje także większy zakres standardów bezprzewodowych, takich jak protokoły 802.11a, b i g i standard szyfrowania WPA (Wi-Fi Protected Access). System IBM obsługuje tylko popularny standard 802.11b i protokół WEP.

4. Wybór technologii i urządzeń dla symulatora

Rysunek 9 przedstawia porównanie poszczególnych technologii sieciowych pod względem odległości oraz szybkości transmisji. Najistotniejsze, z punktu widzenia projektowanej sieci parametry zebrano w tabeli 3.



Rys. 9. Przepustowość oraz zasięg poszczególnych standardów sieci radiowych

Tabela 3. Porównanie standardów sieci bezprzewodowych. Opracowanie własne.

	IrDA	**Bluetooth**	**802.11b**	**802.11g**	**HomeRF**	**HiperLAN/2**
Szybkość	16 mb/s	780 kb/s (do 1 Mb/s)	11 MB/s	54 Mb/s	1 – 2 MB/s	54 Mb/s
Maksymalny zasięg	1 m[1]	100 m[2]	100 m	100 m	50 m	b.d.
rodzaj transmisji	podczerwień	radiowa	radiowa	radiowa	radiowa	radiowa
pasmo lub zakres fal	zakres falowy 850 – 900 nm	2,5 GHz	2,4 GHz	2,4 GHz	2,4 GHz	5 MHz

[1] przy szybkości 75 kb/s – ponad 5m

2 przy zwiększonej mocy transmisyjnej

b.d. – brak danych

4.1. Zalecenia końcowe

Należy rozpatrzyć sprzęt ze standardem 802.11b (11 Mb/s) i 802.11g (54 Mb/s). Urządzenia z zaimplementowanym 802.11g mają zwykle zaimplementowane 802.11b. Poniższa tabela przedstawia zasięgi i przepływności osiągane przez punkty dostępowe Cisco

Tabela 2. Parametry techniczne punktów dostępowych Cisco.

Zasięg Cisco AP 1200(802.11a/b/g) i 1100(802.11b/g)			
802.11g		802.11b	
m	Mb/s	m	Mb/s
indoor			
27	54	48	11
29	48	67	5,5
30	36	82	2
42	24	124	1
54	18		
64	12		
76	9		
91	6		
outdoor			
76	54	304	11
185	18	610	1
396	6		
Zasięg Cisco 350(802.11b)			
indoor			
		40	11
		107	1
outdoor			
		244	11
		610	1

Z uwagi na fakt, iż aplikacja wymaga dużych przepływności proponuje się zastosowanie Access Point (punktu dostępowego) ze standardem 802.11g (54 [Mb/s] – do 27 metrów), z implementacją 802.11b, dla zachowania

(ewentualnej) kompatybilności dla kart 802.11b. Pociąga to za sobą oczywiście zakup kart 802.11g.

Proponowane rozwiązanie to Cisco Aironet 1100 z kartami Cisco PCMCIA.

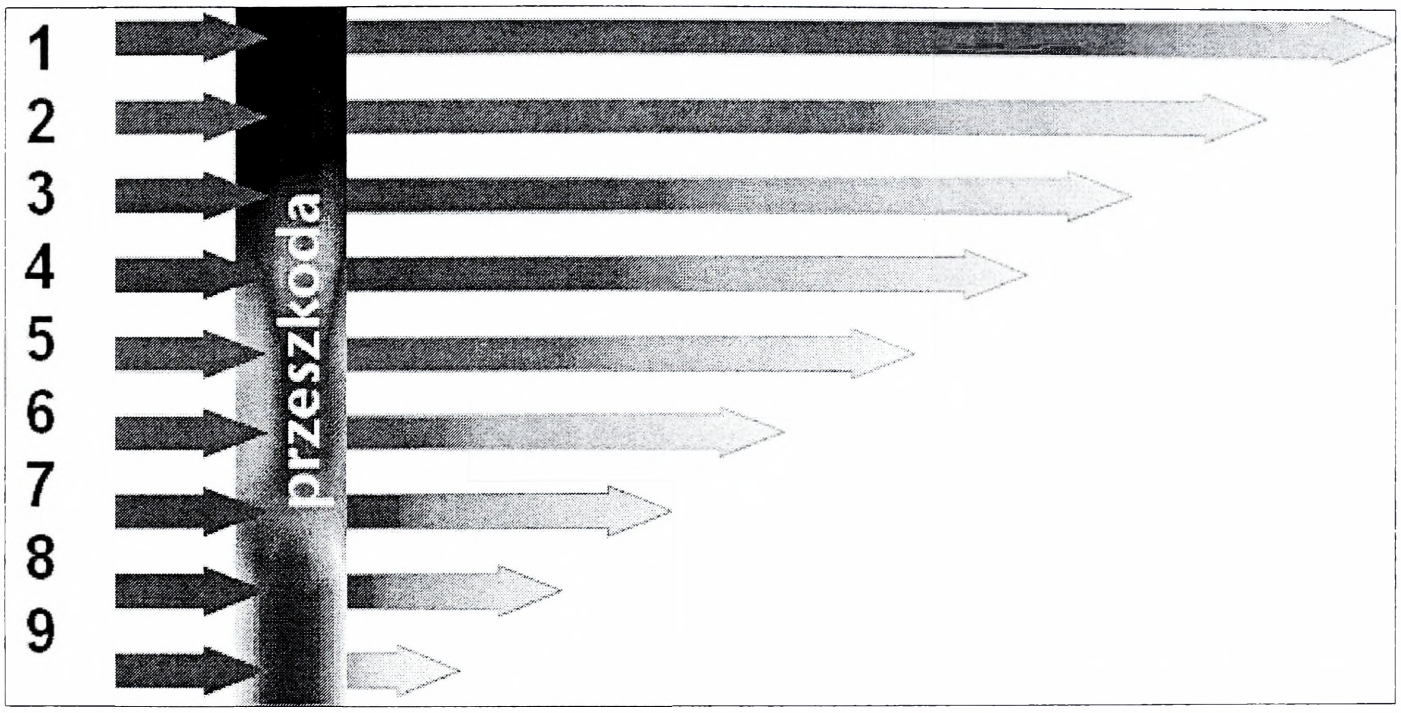
Mając na uwadze wymagania określone na początku niniejszego opracowania oraz możliwości i ograniczenia poszczególnych standardów, proponuje się:

1. Za standard pracy sieci lokalnej przyjąć 802.11g, jednocześnie zapewniając zgodność ze standardem 802.11b.
2. Za tryb pracy przyjąć tryb infrastrukturalny.
3. Stacje robocze (komputery typu laptop) wyposażyć w karty typu PCMCI, zgodne z ww. standardami. (np. 10 szt.)
4. Liczbę punktów dostępowych dostosować do wymiarów budynków. (*Dla potrzeb prezentacji może wystarczyć np. 4 szt.) – dokładnie będzie wiadomo po zapoznaniu się z wymiarami konkretnej sali, przy konkretnych prezentacjach.*

Ponadto, podczas analizowania ewentualnych zastosowań sieci bezprzewodowej należy wziąć pod uwagę następujące wytyczne i zalecenia:

- punkty dostępowe (Access Points) należy instalować wysoko na ścianach lub po sufitem, w celu eliminowania zakłóceń wprowadzanych przez przeszkody, np. meble;
- zasięg fal radiowych jest znacząco ograniczany poprzez zbrojone ściany, sufity oraz drzwi pancerne (metalowe);

- punkty dostępowe oraz karty radiowe powinny pochodzić z oferty jednego producenta;
- przy doborze urządzeń należy uwzględnić konstrukcję budynków, wyposażenie pomieszczeń itp. (por. rys. 10)



Rys. 10. Tłumienie sygnału radiowego w różnych ośrodkach

- **1** Powietrze (brak przeszkód),
- **2** Drewno (ścianka działowa, parkiet),
- **3** Cegła (ścianka działowa, wysoki mur),
- **4** Tworzywa sztuczne (pleksi, panele),
- **5** Szkło (szyby, ścianki działowe),
- **6** Kamień (posadzka, ściana),
- **7** Cement (podłoga, ściana),
- **8** Szyba hartowana (okna),
- **9** Metal, żelbeton (drzwi, stropy, ściany).

4.2. Podsumowanie

Większość rysunków ze względu na wyjątkową czytelność przekazu zaczerpnięto z Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.

Większość treści opracowania powstała na podstawie dostępnych publikacji w 2003 roku oraz najnowszych informacji przekazywanych na konferencjach oraz z Internetu.

Opracowanie to stanowi stabilna podstawę i uzasadnienie do zakupu sprzętu określonego w zadaniu 12 w harmonogramie realizacyjnym symulatora.

Literatura

1. Douglas E. Comer, Sieci komputerowe TCP/IP tom 1, Zasady, protokoły i architektura, WNT, Warszawa 1997.
2. Ryohei Nakatsu, Junichi Hoshino Entertainment Computing Technologies and Applications, nr ISBN: 1-4020-7360-7, Wydawnictwo: KLUWER 2003.
3. Sheldon T., Wielka encyklopedia sieci komputerowych, Wydawnictwo Robomatic, 2001.
4. Słownik informatyki, WNT, Warszawa 1989.
5. Vademecum teleinformatyka cz. I, Wyd. IDG Poland S.A., Warszawa 2001.
6. Vademecum teleinformatyka cz. II, Wyd. IDG Poland S.A., Warszawa 2002.
7. Zdrodowski B., Zych J. Model działań powietrznych, etap I, Model taktycznych działań powietrznych, AON, Warszawa 2002.
8. Zdrodowski B., Zych J. Model działań powietrznych, etap II, Rozpoznanie i zarządzanie zasobami w modelu działań powietrznych, AON, Warszawa 2002.
9. Zdrodowski B., Zych J. Model działań powietrznych, etap III, Teren w modelu działań powietrznych, AON, Warszawa 2003.
10. Zdrodowski B., Zych J. Model działań powietrznych, etap IV, Warunki meteorologiczne w modelu działań powietrznych, AON, Warszawa 2003.

11. Zdrodowski B., Zych J. Symulator operacyjno-taktycznych działań powietrznych - GAMBLER, tom 1, Koncepcja realizacji projektu, AON, Warszawa 2003.

12. Zdrodowski B., Zych J. Symulator operacyjno-taktycznych działań powietrznych - GAMBLER, tom 2, Założenia funkcjonalno-techniczne symulatora operacyjno-taktycznych działań powietrznych, AON, Warszawa 2003.

13. Zdrodowski B., Zych J., Symulator operacyjno-taktycznych działań powietrznych - GAMBLER, tom 3, Wymagania bazy technologicznej i oprogramowania symulatora operacyjno-taktycznych działań powietrznych, AON, Warszawa 2003.

14. Zdrodowski B., Zych J., Projekt fizycznego modelu laboratoryjnego symulatora operacyjno-taktycznych działań powietrznych, Ministerstwo Nauki i Informatyzacji oraz Akademia Obrony Narodowej, Akademia Obrony Narodowej, Warszawa 2003.

15. Zych. J., Model walki sił obrony powietrznej szczebla taktycznego, Rozprawa doktorska, Akademia Obrony Narodowej, Warszawa 2002.

16. Zych J., Computerised Simulation Game, Proceedings of The Regional Conference on Military Communication and Information Systems, Zegrze, Poland, October 8-10 2003.

17. Zych J., Lotnictwo, stulecie, przemiany, Gry wojenne w lotnictwie wojskowym, Fundacja otwartego muzeum techniki, Wrocław, 2003.

18. Zych J., Symulacja procesów logistycznych w grze wojennej, Problematyka normalizacji zapewnienia jakości i kodyfikacji w aspekcie integracji z NATO i Unią Europejską, Instytut Automatyzacji Systemów Dowodzenia i Logistyki Wojskowej Akademii Technicznej, Warszawa 2003.

19. Zych J., Laskowski W., Badanie bezpieczeństwa teleinformatycznego metodą symulacyjną, SECURE 2003, VII konferencja bezpieczeństwa IT, NASK, Warszawa 2003.

20. Zych J., Cybernetyczny aspekt przetwarzania informacji, Przegląd Wojsk Lotniczych i Obrony Powietrznej, nr 12, Poznań 2003.

21. Zych J., Symulacja procesów logistycznych w grze wojennej, Problematyka normalizacji zapewnienia jakości i kodyfikacji w aspekcie integracji z NATO i Unią Europejską, Instytut Automatyzacji Systemów Dowodzenia i Logistyki Wojskowej Akademii Technicznej, Warszawa 2003.

22. Zych J., Computerised Simulation Game, 5th NATO Regional Conference on Military Communication and Information Systems 2003 Capturing new CIS Technologies, Zegrze, Poland 2003.

23. Zych J., Meteorological aspects of the Gambit War Game, V International Symposjum on Military Meteorology, Poznań, Poland 2003.

24. Zych J., Badanie bezpieczeństwa teleinformatycznego metodą symulacyjną, SECURE 2003, VII konferencja bezpieczeństwa IT, Warszawa 2003, *(jako współautor)*.

25. Zych J., Gry wojenne w lotnictwie wojskowym, Lotnictwo Stulecie Przemiany, Fundacja Otwartego Muzeum Techniki, Wrocław 2003.

3092

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 57092
Akademii Obrony Narodowej