STUDIA INFORMATICA 2002
Volume 23 Number 3 (50)

Kazimierz LAL
Politechnika Rzeszowska, Katedra Informatyki i Automatyki

# RADIOWY ETHERNET JAKO NOŚNIK INFORMACJI W SYSTEMACH STEROWANIA OBIEKTAMI MOBILNYMI

**Streszczenie.** Praca omawia wybrane zagadnienia dotyczące problematyki transmisji danych za pomocą systemów bezprzewodowych, w szczególności tzw. radiowego Ethernetu, bazującego na unormowaniach IEEE 802.11 i 802.11b. Jest wstępem do planowanego wykorzystania standardów stosowanych w sieciach lokalnych WLan, w systemach sterownia obiektami mobilnymi.

# RADIO ETHERNET AS INFORMATION CARRIER IN CONTROL SYSTEMS FOR MOBILE OBJECTS

**Summary.** The paper discusses selected issues of data transmission by means of wireless systems, in particular the so-called radio Ethernet, based on IEEE 802.11 and 802.11b standards. It is an introduction to planned utilization of the WLan standards in control systems for mobile object.

## 1. Protokoły dostępu w sieciach bezprzewodowych

Istotnym problemem w sieciach bezprzewodowych (WLan), warunkujących możliwość zastosowania określonych protokołów dostępu do warstwy fizycznej (wg modelu ISO-OSI) jest „konfiguracja połączeń". Jeżeli sieć ma konfigurację gwiazdy (jedynie stacja centralna ma łączność ze stacjami lokalnymi) – to można stosować odpytywanie. W przypadku gdy wszystkie stacje posiadają wzajemną łączność, można wykorzystać protokoły z żetonem lub protokoły rywalizujące o medium.

### 1.1. Dostępność stacji

W praktyce, z uwagi na różne zakłócenia należy uwzględniać możliwość utraty części połączeń i wtedy przewidzieć zachowanie całego systemu.

W pracach [7, 8] specyfikuje się najważniejsze z takich problemów.

Są to:

Zjawisko ukrytej stacji.

Zjawisko odkrytej stacji.

Interferencje pomiędzy stacjami.

Efekt przechwytywania.

W pierwszym przypadku analizowana stacja znajduje się w zasięgu każdej stacji odbierającej sygnały, ale istnieją takie stacje nadające, których sygnałów ona nie odbiera. W dogłębnej analizie omawianego zjawiska wyróżnia się bardziej szczegółowe sytuacje – zagadnienie ukrytego nadajnika i/lub ukrytego odbiornika.

Przypadek przeciwny, gdy wyróżniona stacja znajduję się w zasięgu dowolnej stacji nadającej i nie wszystkie stacje odbierające ją „widzą", nazywany jest zjawiskiem odkrytej stacji. Podobnie jak w zjawisku ukrytej stacji można również tutaj wyróżnić zjawisko odkrytego nadajnika i odkrytego odbiornika.

Efekt interferencji pojawia się wtedy, gdy określona stacja znajduje się poza zasięgiem zarówno nadajnika, jak i odbiornika, jednak na tyle blisko, że zakłóca transmisje pomiędzy nimi.

Przechwytywanie występuje w sieciach, wymieniających komunikaty za pomocą fal radiowych. Występuje ono wtedy, gdy do odbiornika docierają co najmniej dwa sygnały o różnej mocy w tym samym czasie. Wtedy najczęściej sygnał o największej mocy jest odbierany poprawnie, a pozostałe zagłuszane.

### 1.2. Protokoły dostępu [7, 8]

Wyspecyfikowane wyżej problemy mają istotny wpływ na poprawność funkcjonowania sieci z dostępem sterowanym, jak i sieci kolizyjnych. Z uwagi na temat niniejszej pracy istotne jest szczegółowe przeanalizowanie ograniczeń dotyczących sieci kolizyjnych, bazujących na falach radiowych. W pewnym uproszczeniu można stwierdzić, że ograniczenia dostępności uniemożliwiają wykorzystanie klasycznych mechanizmów wykrywania kolizji (np. CSMA/CD z Ethernetu przewodowego). W praktyce stosuje się protokoły z mechanizmem potwierdzeń lub dodatkowego nasłuchu.

### *1.2.1. Protokół CSMA/CA*

W protokole CSMA/CA wykrywanie kolizji realizowane jest wg następującego algorytmu. Stacja nadawcza rozpoczyna nadawanie wtedy, gdy oceni, że kanał transmisyjny jest wolny. W przeciwnym przypadku czeka i sprawdza zajętość.

Stacja odbiorcza po odebraniu ramki wysyła potwierdzenie pozytywne (poprawny odbiór) lub potwierdzenie negatywne (wystąpiła kolizja lub inny błąd). Stacja nadawcza oczekuje na potwierdzenie pozytywne. Brak potwierdzenia w określonym czasie lub potwierdzenie negatywne są tożsame – należy dokonać retransmisji. Istnieje wiele podwersji protokołu CSMA/CA, np. tzw. protokoły bez wymuszenia transmisji i z wymuszeniem transmisji.

W pierwszym – po każdej kolizji – stacja nadawcza wznawia transmisję po losowo wybranym czasie. W drugim – po pierwszej kolizji – stacja nadawcza określa moment zwolnienia kanału, po czym od tego momentu dzieli czas na szczeliny o długości równej podwojonemu maksymalnemu czasowi propagacji ramki i z pewnym prawdopodobieństwem próbuje rozpocząć transmisję na początku kolejnej szczeliny.

### *1.2.2. Protokół BTMA*

Przez podział kanału podstawowego na dwa podkanały: komunikatów oraz zajętości twórcy protokołu BTMA podjęli próbę rozwiązania problemu ukrytych stacji.

Każda stacja, odbierając dane w podkanale komunikatów, wysyła sinusoidalny sygnał w podkanale zajętości. Każda stacja przed nadaniem swojej ramki sprawdza stan podkanału zajętości. Cisza w tym podkanale zezwala na transmisję, w przeciwnym przypadku transmisja jest odkładana na później. Cechami charakterystycznymi dla omawianego protokołu jest zmniejszenie szerokości kanału do transmisji danych, możliwość łatwego zablokowania całej struktury przy błędnej generacji sygnału zajętości oraz wrażliwość na różnice propagacji sygnałów radiowych na różnych częstotliwościach nośnych.

### *1.2.3. Protokoły MACA i MACAW*

Problemy z transmisją przy występowaniu stacji odkrytych i zakrytych doprowadziły do powstania protokołu MACA, w którym wykorzystuje się dodatkowe ramki sterujące. Stacja nadawcza generuje ramki sterujące RTS, a stacja odbiorcza CTS. Takie postępowanie pozwala na wyeliminowanie większości problemów, jakie rodzi występowanie sieci stacji odkrytych i/lub ukrytych. Nie zapobiega jednak wszystkim kolizjom.

Protokół MACAW jest w zasadzie rozwinięciem MACA. Wprowadza dodatkowe ramki sterujące (DS- Data Sending, ACK-ACKnowledge, RRTS-Request for RTS), co umożliwia lepsze rozwiązanie problemów transmisji.

### *1.2.4. Protokóły FAMA*

Protokoły FAMA w swoich zasadach działania są pewną syntezą protokołów MACA, MACAW, SRMA, MSAP i BRAM. Wykorzystują mechanizm wykrywania sygnału nośnego, wymiany ramek sterujących i rezerwację dynamiczną nośnika. Całość transmisji realizowana jest w jednym wspólnym kanale. Naturalny w takim przypadku problem kolizji rozwiązano przez wprowadzenie sztywnych zależności czasowych. W efekcie ramki z danymi transmitowane są (w zasadzie) bez kolizji.

### *1.2.5. Protokół BAPA*

Zaprezentowane wyżej protokoły ze wstępną wymianą komunikatów sterujących nie rozwiązują problemu interferencji. Z tym problemem zmierza się protokół BAPA, w którym przez wyróżnienie kanału danych i kanału sterującego o odpowiednio większym zasięgu doprowadzono do sytuacji, w której stacje interferujące w kanale danych stają się stacjami odkrytymi lub ukrytymi w kanale sterującym. W protokole używa się pięciu ramek sterujących (RTS, CTS, DS., ACK i NCTS-Not Clear To Send).

## 2. Sieci bezprzewodowe standardu IEEE 802.11 i 802.11b

Jak wszystkie standardy serii IEEE 802.XX również IEEE 802.11(b) [1, 2, 4, 5, 6, 7, 8] obejmuje dwie najniższe warstwy modelu ISO-OSI. W warstwie fizycznej definiuje dwa typy transmisji FHSS i DSSS oraz sposób kodowania CCK. Warstwa łącza danych analogicznie jak np. w Ethernecie 10BaseT podzielona jest na dwie podwarstwy LLC i MAC.

### 2.1. Urządzenia standardu IEEE 802.11(b)

Norma 802.11 definiuje dwa różne komponenty sieci – stację radiową i punkt dostępu AP. Pierwszy z nich to najczęściej komputer klasy PC wyposażony w odpowiednią kartę sieciową (NIC) z interfejsem 802.11b, zrealizowaną w formie PC-CARD, karty PCI lub ISA. W praktyce, z uwagi na wysokie koszty procedur homologacji urządzeń radiowych, większość producentów produkuje tylko PC-CARD w standardzie 802.11b i odpowiednie adaptery magistrali PCIMCIA/PCI, PCIMCIA/ISA (produkt zanikający), PCIMCIA/USB. Punkt dostępu – to autonomiczne urządzenie zbudowane z podzespołów radiowych (nadajnik, odbiornik, zestaw anten), interfejsu sieci kablowej oraz mostu łączącego świat sieci kablowej i radiowej. Punkt dostępu – to stacja główna sieci radiowej, zapewniająca dostęp stacjom radiowym.

### 2.2. Tryby dostępu w IEEE 802.11(b)

Omawiane normy precyzują dwa tryby pracy – tzw. tryb infrastruktury i tryb doraźny. W pierwszym, w sieci występuje co najmniej jeden punkt AP, połączony do stacjonarnej sieci kablowej oraz zestaw komunikujących się z nim stacji radiowych. Jeżeli w sieci jest tylko jeden punkt AP – to w szczegółowej nomenklaturze IEEE 802.11 określana jest ona jako BSS. Zestaw kilku współpracujących podsieci BSS nazywany jest siecią o konfiguracji ESS.

Drugi tryb – doraźny – IBSS, realizowany w formie sieci partnerskiej, gdy nie ma stacji AP, a stacje radiowe mogą komunikować się każda z każdą. Z punktu widzenia protokołów warstwy łącza danych (ISO-OSI) tryby te określane są jako: (pierwszy) „ze scentralizowaną funkcją koordynacji" i (drugi) „z rozproszoną funkcją koordynacji".

### 2.3. Warstwa fizyczna IEEE 802.11

W ramach norm IEEE 802.11(b) zdefiniowano trzy techniki transmisji. Dwie techniki radiowe i jedną, bazującą na podczerwieni.

W celu zapewnienia odpowiedniej przepustowości opracowano kilka specjalnych sposobów transmisji. Obecnie dominuje standard DSSS (dla 802.11b), a w mniejszym zakresie jest używany FHSS. Z uwagi na zalecenia dotyczące podziału pasma radiowego transmisje realizowane są w tzw. paśmie wolnym (nie licencjonowanym wg FCC-USA/ETSI-EU/MKK-JAPAN), w zakresie mikrofal, czyli paśmie 2.4 GHz tzw. ISM.

Jest to pasmo dość mocno zakłócane przez urządzenia powszechnego użytku, np. kuchenki mikrofalowe, dlatego obecnie pracuje się na unormowaniami, które pozwolą w przyszłości wykorzystywać w sieciach radiowych pasma obecnie chronione, o większych częstotliwościach (np. 5.2 GHz, 17 GHz itd.).

Technika DSSS sprowadza się do kluczowania sygnału danych szybkozmienną sekwencją pseudolosową. W praktyce oznacza to, że oryginalny sygnał danych podawany jest na bramkę XOR, w której na drugie wejście podawane są specjalnie przygotowane sekwencje bitów o znacznie większej częstotliwości taktowania (tzw. chipów). Z wyjścia bramki sygnał trafia do modulatora i w eter – w jeden z trzech niezależnych szerokopasmowych $\Delta f$=25MHz (11 Mb/s) kanałów, w paśmie 2.4 GHz (np. o sekwencji 1,6,11 albo 2,7,12). Dla postronnego odbiornika tak przetworzony sygnał przypomina szum. Należy tutaj podkreślić, że szybkość sygnalizacji (szybkość związana z zajętym pasmem) jest znacznie większa od szybkości przesyłania danych.

W omawianej sieci stacja odbiorcza prowadzi nasłuch w całym dopuszczalnym paśmie. Po odebraniu sygnału wykonuje proces demodulacji i powtórnego kluczowania z taką samą

sekwencją pseudolosową jak nadajnik, ale wytworzoną przez lokalny generator sekwencji pseudolosowych.

DSSS zapewnia dobrą odporność na zakłócenia, z uwagi na nadmiarowość sygnalizacji umożliwia (w pewnym zakresie) odtworzenie sygnałów o poziomie takim samym jak szumy. W warunkach dobrej łączności technika DSSS zapewnia uzyskanie większych szybkości transmisji (5,5 oraz 11 Mb/s) i dlatego jest podstawą nowszego standardu IEEE 802.11b.

Technika FHSS posługuje się piętnastoma (z 82 dostępnych) wąskopasmowymi kanałami transmisyjnymi 1,6 Mb/s. Podczas transmisji dany kanał wykorzystywany jest przez 100-200 ms. Później wykonywany jest przeskok na kolejny kanał, o numerze określonym przyjętą sekwencją pseudolosową.

FHSS pozwala na pracę w jednym obszarze do 15 stacji AP, przez sekwencje skoków jest odporna na selektywnie występujące zakłócenia i trudna do podsłuchu. Ma jednak znaczącą wadę – małą szybkość transmisji.

Szybka komunikacja z wykorzystaniem promieniowania podczerwonego IR, transmitowanego w wolnej przestrzeni, ciągle należy do technologii przyszłości. Mimo bez trudu osiąganych szybkości 155 Mb/s, czy 622 Mb/s ciągle jest produktem eksperymentalnym.

## 2.4. Warstwa fizyczna IEEE 802.11b

Jak już wspomniano, na bazie techniki DSSS opracowano nowy standard 802.11b, który ma kilka charakterystycznych cech:

udostępnia dwie nowe szybkości transmisji 5,5 Mb/s i 11 Mb/s,

jest kompatybilny z IEEE 802.11-DSSS,

nie współpracuje z IEEE 802.11-FHSS.

W nowej warstwie fizycznej stosuje się bardziej zaawansowane techniki kodowania – w tym technikę CCK, która wykorzystuje kodowanie wielowartościowe w postaci sekwencji 64 8-bitowych słów kodowych tak dobranych, że nawet w obecności znacznych zakłóceń oraz interferencji wielościeżkowych transmisja jest poprawna. W przypadku jednak, gdy przekłamania przekraczają określony próg – standard IEEE 802.11b (sieci WLAN 802.11b) za pomocą mechanizmu dynamicznej zmiany prędkości zmniejsza swoją szybkość sygnalizacji, co często (przy dużych zakłóceniach) poprawia szybkość transmisji danych. Mechanizm zmiany szybkości sygnalizacji reaguje przeciwnie, gdy poziom przekłamań maleje – po prostu sukcesywnie zwiększa szybkość – do maksymalnej.

Teoretycznie zmiany prędkości transmisji są autonomiczną funkcją warstwy fizycznej, a więc nie mogą w nie ingerować warstwy wyższe i użytkownik.

### 2.5. Protokoły warstwy łącza danych IEEE 802.11(b) [4]

Warstwa łącza danych (model ISO-OSI) w IEEE 802.11 podzielona jest na kilka dodatkowych podwarstw. Bezpośrednio nad warstwą fizyczną funkcjonuje protokół podwarstwy MAC tzw. DFWMAC. Jest on niezależny od warstwy fizycznej, a więc oferuje takie same zasady dostępu dla DSSS, FHSS i IR. Protokół DFWMAC określa wspomniane wcześniej dwa tryby pracy sieci:

tryb z rozproszoną funkcją koordynacji – DCF,

tryb ze scentralizowaną funkcją koordynacji – PCF

oraz protokół udostępniający medium transmisyjne – częściowo zmodyfikowany protokół CSMA/CA.

Algorytm kontrolny protokołu CSMA/CA nosi nazwę CCA i dla trybu DCF pracuje według schematu – „zanim zaczniesz nadawać dane, musisz posłuchać". Tak więc gotowa do nadawania stacja prowadzi najpierw nasłuch, sprawdzając, czy ktoś inny nie wymienia danych. Jeżeli w określonym czasie PIFS nie wykryje żadnego ruchu w nośniku, przełącza się w tryb gotowości do nadawania i następnie czeka dodatkowo jedną szczelinę czasową – w sumie 128 μs. Jeżeli dalej trwa cisza – to stacja rozpoczyna transmisję swoich danych. W praktyce stan medium transmisyjnego określa się przez pomiar energii odbieranej z anteny lub fotoodbiornika.

W trybie PCF(ze stacjami AP) taki algorytm nie musi pracować poprawnie – po prostu w takiej konfiguracji mogą występować tzw. ukryte węzły, a wtedy brak sygnału na wejściu odbiornika danej stacji nie jest tożsamy z brakiem nadawania przez stację ukrytą. W takim przypadku ruch jest kierowany przez AP.

Przed koleją sesją transmisji AP generuje sygnał zajętości nośnika, aby w ten sposób zasygnalizować początek danej sesji. Następnie wysyła do wszystkich stacji podrzędnych sygnał zezwalający na nadawanie. Obsługa zgłoszeń wykorzystuje mechanizm tzw. superramki, wewnątrz której wydzielono dwa odcinki czasu – pierwszy dla transmisji kolizyjnej (stacje rywalizują, aby wpisać się na listę do obsługi przez AP) i drugi dla transmisji danych – sterowanej przez AP (bezkolizyjny o zmiennej długości). Transmisja między stacją podrzędną a punktem dostępu odbywa się na zasadzie odpytywania. Możliwa jest również wymiana danych bezpośrednio pomiędzy stacjami należącymi do BSS (jednej komórki), ale taka transmisja jest również inicjowana i kontrolowana przez AP.

W protokole DFWMAC określono trzy poziomy priorytetów :

najwyższy, dla przesyłania odpowiedzi natychmiastowych, w tym potwierdzeń,

średni, dla realizacji protokołu odpytywania PCF,

najniższy, dla realizacji protokołu DCF.

## 2.6. Ramki

Standard 802.11 wyróżnia trzy podstawowe typy ramek:

- ramki danych,
- ramki kontrolne,
- ramki służbowe (zarządzające).

## 2.7. Wędrowanie w sieci 802.11 z wieloma AP

Standard 802.11 nie definiuje, jak powinno przebiegać wędrowanie stacji radiowej, a jedynie definiuje podstawowe narzędzia, takie jak skanowanie aktywne, pasywne, procesy przełączania, gdy wędrująca stacja przełącza się do kolejnego AP. Proces dynamicznego łączenia i przełączania pomiędzy AP pozwala na budowanie sieci o stosunkowo dużej rozległości.

## 2.8. Bezpieczeństwo

Sieci bezprzewodowe, w szczególności radiowe, generują sygnały, które mogą wykraczać poza przyjęty obszar użytkowy. Ten stan prowadzi do wielu problemów. Systemy radiowe są podatne na zakłócenia zewnętrzne (w tym sabotaż), generują zakłócenia, które mogą negatywnie wpływać na działanie innych urządzeń, są łatwe do podsłuchania. W omawianym standardzie 802.11(b) w celu zapewnienia odpowiedniego poziomu bezpieczeństwa można stosować metody szyfrowania z tzw. kluczem dzielonym (WEP). Należy zauważyć, że IEEE nie określa zasad rozdzielania kluczy dla każdej stacji.

## 2.9. Konkurencyjne standardy bezprzewodowych sieci lokalnych

Systemy bezprzewodowe obecnie przeżywają burzliwy rozwój. Wiele przyjętych w przeszłości założeń nie sprawdza się. Dlatego oprócz omawianych standardów IEEE 802.11(b) istnieją inne.

W ramach projektu Home Radio Frequency powstał system SWAP, który łączy cyfrowy standard telefonii bezprzewodowej DECT z systemem przesyłania danych 802.11.

Europejski Komitet Normalizacji ETSI tworzy standardy HiPeRLAN, HiPeRACCESS i HiPeRLINK o dużej przepustowości, przeznaczone do wykorzystania w aplikacjach multimedialnych.

Jeden z pionierów systemów radiowych – PROXIM promuje system OpenAir.

## 3. Wstępne badania urządzeń standardu 802.11(b)

Przeprowadzono wstępne badania dostępnych na rynku urządzeń [1,2,3,4] pod kątem zastosowania ich w systemach sterowania obiektami mobilnymi. Przeprowadzono eksperymenty dotyczące zasięgu wewnątrz pomieszczeń, w przestrzeni otwartej, w przestrzeni zabudowanej, w obecności zakłóceń generowanych przez silniki elektryczne prądu stałego, silniki spalinowe z zapłonem iskrowym oraz przez obiekty energetyczne – stacje transformatorowe i linie średniego napięcia. Uzyskane rezultaty, choć bardzo wstępne, pozwalają na pewne uogólnienia. W otoczeniu obiektów energetycznych transmisja w standardzie DSSS praktycznie nie jest możliwa. Standard FHSS pozwala na komunikację, ale uzyskiwane średnie szybkości transmisji w konkretnych przypadkach – to często kilkaset bajtów na sekundę. Komutatorowe silniki prądu stałego małej mocy (ok.400[W]), po zastosowaniu dość prostego filtru oraz ekranu przeciwzakłóceniowego, nie wpływają istotnie na działanie stacji radiowych wtedy, gdy odległość pomiędzy stacją i silnikiem przekracza 0,5[m]. Zakłócenia generowane przez współczesne silniki samochodowe oraz motocyklowe nie wpływają istotnie na pracę stacji radiowej przy odległościach większych od 1[m]. Znacznym problemem jest korzystanie z sieci radiowych w pomieszczeniach fabrycznych.

Żaden z czterech zestawów testowanych urządzeń nie pozwalał na efektywne wędrowanie stacji radiowych pomiędzy kolejnymi stacjami bazowymi AP. W miejscach jednakowo oddalonych od dwu stacji czas transmisji testowego pliku o długości 100kB wydłużał się o 20-40 % w stosunku do stanu, gdy pracowała tylko jedna stacja.

## 4. Wnioski

Analiza teoretyczna i wstępne badania systemów bezprzewodowych WLan nie pozwalają na jednoznaczną ogólną opinię co do ich przydatności w systemach sterowania obiektami mobilnymi. Można jednak postawić tezę, że w określonych konkretnych warunkach można dobrać takie konfiguracje sprzętu (w tym anten) i tak rozmieścić stacje bazowe, że można zbudować efektywny system transmisji sygnałów do sterowania nadrzędnego obiektami mobilnymi. Planowane jest wykonanie odpowiednich badań i eksperymentów.

## LITERATURA

1. 3Com Corporation: White Paper. www.3com.com
2. BreezeNet PRO 11 Series, User's Guide. BrezzeCOM Ltd. 1999.

3. Compex AirNet. User's Guide – 2000.
4. Intel: IEEE 802.11b High Rate Wireless Area Networks. Intel Corp. 2000.
5. Intel: IEEE 802.11a. Intel Corp.2001.
6. PCKurier. Nr 23/2000.
7. Pączek M, Sieraczyński G.: Systemy radiowego Ethernetu jako nośnik do pracy zdalnej w sieciach komputerowych. Praca magisterska PRz-2001.
8. Zieliński B.: Bezprzewodowe sieci komputerowe. Wydawnictwo Helion, Gliwice 2000.

Recenzent: Dr inż. Bartłomiej Zieliński

Wpłynęło do Redakcji 29 marca 2002 r.

**Abstract**

One of the major problems in mobile-object control systems is the data transmission between an external computer and an on-board controller. The author proposes to utilize the standard wireless interface, IEEE 802.11(b), as used in LANs networks, for such communication.

The subsequent sections deal with general problems of wireless station accessibility, typical communication protocols and selected issues of the physical structure and logical organization of the IEEE 802.11 and 802.11(b) interfaces. The competitive standards of wireless networks – ETSI – HiPeRLAN, HiPeRACCESS and HiPeRLINK are also mentioned. The final part of the paper describes the results of initial tests available on the market of the 802.11b standard equipment in respect to their potential utilization in an industrial environment, where quite significant electromagnetic interference may be emitted by transformers, electric motors and IC engines, as well as electromagnetic field disturbances are caused by the effects of grounded conducting elements.