ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: INFORMATYKA z. 36 Nr kol. 1414

Bartłomiej ZIELIŃSKI
Politechnika Śląska, Instytut Informatyki

PROTOKOŁY DOSTĘPU DO ŁĄCZA W SIECIACH BEZPRZEWODOWYCH

Streszczenie. Omówiono problematykę rywalizacyjnych protokołów dostępu do łącza dla sieci bezprzewodowych. Opisano wybrane protokoły dostępu do łącza dla tych sieci.

MEDIUM ACCESS PROTOCOLS IN WIRELESS NETWORKS

Summary. The problem of random MAC protocols in wireless networks has been described. Selected protocols for such networks have been characterized.

1. Wprowadzenie

Łączność bezprzewodowa jest coraz popularniejszym sposobem wymiany informacji. Świadczy o tym m. in. duża i stale rosnąca liczba użytkowników telefonów komórkowych. Niemal wszystkie komputery przenośne są wyposażone w środki łączności bezprzewodowej. Powstają w ten sposób sieci bezprzewodowe, także sieci lokalne.

W przewodowych sieciach lokalnych zagadnieniem o dużej wadze jest problem dostępu do współdzielonego łącza transmisyjnego. Również i w sieciach bezprzewodowych występuje potrzeba wprowadzenia efektywnego sposobu przydzielania łącza poszczególnym stacjom sieci. Różnice, jakie dzielą technikę transmisji przewodowej i bezprzewodowej, powodują jednak, że sieci bezprzewodowe potrzebują innych, zmodyfikowanych metod dostępu do łącza. Potrzeba ta uwidacznia się szczególnie w sieciach, wykorzystujących protokoły rywalizacyjne.

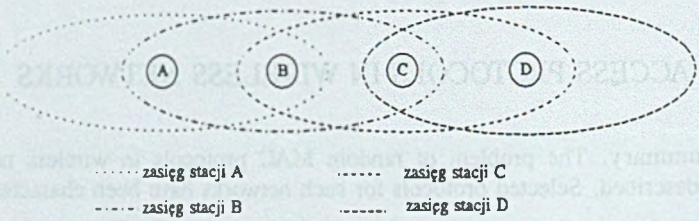
2. Geneza problemu

Jak już wspomniano, sieci bezprzewodowe wykazują szereg różnic w stosunku do sieci przewodowych [1]. Z punktu widzenia rywalizacyjnych protokołów dostępu do łącza najistotniejszymi problemami są [2]:

- zjawisko ukrytej stacji,
- zjawisko odkrytej stacji,
- interferencje,
- efekt przechwytywania.

2.1. Zjawisko ukrytej stacji

Zjawisko ukrytej stacji (ang. *hidden terminal*) [2, 3] może wystąpić, kiedy nie wszystkie stacje sieci mają bezpośrednią łączność, jak pokazano na rys. 1. Stacja jest ukryta, jeżeli znajduje się w zasięgu stacji odbierającej dane, ale jest poza zasięgiem stacji nadającej [4].



Rys. 1. Ilustracja zagadnienia problemu stacji ukrytej i odkrytej
Fig. 1. Hidden and exposed terminal scenario

Stacja A nadaje do stacji B. Ponieważ stacje A i C znajdują się poza swoim zasięgiem, transmisja ta nie zostanie wykryta w stacji C, która wobec tego przyjmuje, że łącze jest wolne i może rozpocząć transmisję do stacji B lub D. Transmisja ta powoduje w stacji B kolizję z danymi ze stacji A, co powoduje spadek ogólnej przepustowości łącza wskutek konieczności retransmisji. Zjawisko ukrytej stacji ilustruje rys. 2.

Rys. 2. Zjawisko ukrytej stacji
Fig. 2. Hidden terminal scenario

W ramach zjawiska ukrytej stacji wyróżnia się ukryte nadajniki i ukryte odbiorniki [4]. Rozróżnienie to możliwe jest w sieciach, w których wysłanie ciągu danych poprzedzone jest wysłaniem informacji sterującej, oznaczającej zamiar nadawania (np. ramka RTS, ang.

Request To Send). Jeżeli adresat tej ramki może odbierać dane, sygnalizuje to nadawcy (np. ramką CTS, ang. *Clear To Send*).

2.1.1. *Ukryty nadajnik*

Zjawisko ukrytego nadajnika występuje, kiedy stacja ukryta (stacja C na rys. 2) ma dane do wysłania. Ponieważ stacja ta nie odbiera stacji A, stacja B powinna powiadomić stację C, że zamierza przyjmować dane ze stacji A.

2.1.2. *Ukryty odbiornik*

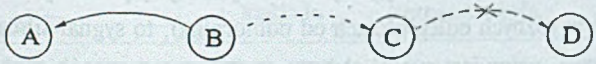
Zjawisko ukrytego odbiornika występuje, kiedy stacja ukryta (stacja C na rys. 2) jest adresatem informacji, wysyłanej ze stacji D. Stacja D nadaje do C ramkę RTS, jednakże stacja C nie może wysłać w odpowiedzi ramki CTS, ponieważ spowodowałoby to kolizję w stacji B. Brak takiej ramki może świadczyć o tym, że:

- stacja C wstrzymuje transmisję,
- ramka RTS stacji D uległa kolizji w stacji C,
- ramka CTS stacji C uległa kolizji w stacji D,
- stacja C jest wyłączona.

W każdym z powyższych przypadków zachowanie stacji D winno być inne. Stacja C musi zatem wysłać do stacji D informację, że wstrzymuje transmisję; informacja ta musi zostać przesłana w osobnym kanale.

2.2. Zjawisko odkrytej stacji

Zjawisko odkrytej stacji (ang. *exposed terminal*) [2, 3] także może wystąpić, kiedy nie wszystkie stacje mają bezpośrednią łączność (rys. 1). Stacja jest odkryta, kiedy znajduje się w zasięgu nadawcy informacji, ale poza zasięgiem odbiorcy [4]. Stacja B nadaje do stacji A. Ponieważ stacje B i C znajdują się w swoim zasięgu, transmisja jest wykryta w stacji C, która wobec tego przyjmuje, że łącze jest zajęte i wstrzymuje transmisję do stacji D. Transmisja ta nie spowodowałaby jednak w stacji A kolizji z danymi ze stacji B, gdyż stacje A i C znajdują się poza swoim zasięgiem. Powoduje to spadek ogólnej przepustowości łącza wskutek zbędnego wstrzymywania transmisji. Zjawisko odkrytej stacji ilustruje rys. 3.



Rys. 3. Zjawisko odkrytej stacji
Fig. 3. Exposed terminal scenario

W ramach zjawiska odkrytej stacji wyróżnia się odkryte nadajniki i odkryte odbiorniki [4]. Rozróżnienie to możliwe jest w sieciach, w których wysłanie ciągu danych poprzedzone jest wymianą ramek sterujących RTS i CTS.

2.2.1. Odkryty nadajnik

Zjawisko odkrytego nadajnika występuje, kiedy stacja odkryta (stacja C na rys. 3) ma dane do wysłania do stacji D. Informacje przesyłane z C do D nie powodują wprawdzie kolizji z transmisją z B do A, jednak odpowiedzi stacji D mogą ulec kolizji z informacjami wysyłanymi z B. Ponieważ niemożliwa jest prawidłowa wymiana ramek sterujących między C i D, stacja C wstrzymuje transmisję danych.

2.2.2. Odkryty odbiornik

Zjawisko odkrytego odbiornika występuje, kiedy stacja odkryta (stacja C na rys. 3) jest adresatem informacji ze stacji D. Stacja D wysyła ramkę RTS, który w stacji C ulega kolizji z danymi z B. Brak ramki CTS ze stacji C można interpretować na kilka sposobów, podobnie jak w przypadku ukrytego odbiornika. Stacja C powinna poinformować, że jest odkrytym odbiornikiem, jednak nie może tego uczynić, gdyż nie docierają do niej żadne ramki sterujące.

2.3. Interferencje

Stacja powoduje interferencję (zakłócenia transmisji), jeżeli jest poza zasięgiem zarówno nadajnika, jak i odbiornika, jednak wystarczająco blisko, aby zakłócać transmisję między nimi [4]. Stacje zakłócające powinny wstrzymać nadawanie, jeżeli inna transmisja jest w toku. W przeciwieństwie jednak do zjawisk ukrytej i odkrytej stacji ani nadajnik, ani odbiornik nie jest w stanie poinformować stacji interferującej o fakcie zakłócania przebiegającego przesyłu informacji.

2.4. Efekt przechwytywania

Efekt przechwytywania (ang. *capture effect*) [5, 6] występuje w sieciach radiowych. Jeżeli do odbiornika docierają dwa sygnały o różnej mocy (np. nadajniki mają różną moc lub są usytuowane w różnych odległościach od odbiornika), to sygnał silniejszy może zostać odebrany prawidłowo, natomiast sygnał słabszy zostaje w ten sposób zagłuszony. Powoduje to, że z dwóch ramek ulegających kolizji jedna może zostać odebrana bezbłędnie. Efekt ten poprawia zatem wykorzystanie kanału transmisyjnego [6].

Negatywnym skutkiem efektu przechwytywania jest niemożność prowadzenia nasłuchu łącza podczas nadawania, jak ma to miejsce w niektórych sieciach przewodowych (np.

Ethernet). W związku z tym niemożliwe jest wykrywanie kolizji podczas nadawania ramki. Dlatego też w celu wykrycia kolizji (a przy okazji i innych nieprawidłowości transmisji) stosuje się mechanizm potwierdzeń. Ponieważ kolizja powoduje błąd transmisji ramki, brak potwierdzenia pozytywnego bądź też potwierdzenie negatywne można uznać za sygnalizację kolizji; być może dlatego w literaturze (np. [7, 8]) można znaleźć informację, że w sieciach bezprzewodowych wykorzystywany jest mechanizm CSMA/CD, znany z sieci Ethernet.

Wykrywanie kolizji jest natomiast możliwe w sieciach, w których medium transmisyjnym jest podczerwień rozproszona [9].

3. Przegląd protokołów dostępu do łącza

W sieciach bezprzewodowych wykorzystuje się wiele rywalizacyjnych protokołów dostępu do łącza. Najstarsze z nich cechują się dużą prostotą, ale i niewielką efektywnością. Dlatego też obecnie stosuje się bardziej zaawansowane metody, dzięki czemu efektywność wykorzystania kanału transmisyjnego jest znacznie większa.

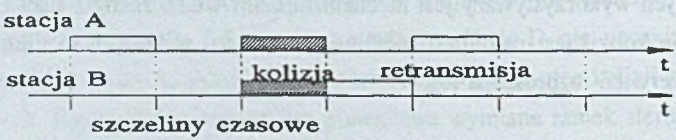
3.1. Protokoły Aloha

Najstarszym i najszerzej znanym protokołem dostępu do łącza dla sieci bezprzewodowej jest protokół stosowany w sieci Aloha [5, 10]. Sieć ta składa z komputera dużej mocy, wyposażonego w stację centralną, oraz dużej liczby terminali, do których dołączone są stacje lokalne. Transmisja ze stacji lokalnej może się rozpocząć kiedykolwiek, niezależnie od stanu łącza, jeżeli tylko dana stacja ma skompletowaną ramkę do wysłania. W związku z tym w sieci następuje wiele kolizji między ramkami wysyłanymi przez różne stacje. Ponieważ w sieci Aloha stacja centralna wysyła potwierdzenia poprawnego odebrania ramki, brak takiego potwierdzenia w określonym czasie może świadczyć o kolizji ramek; ramka niepotwierdzona jest wówczas nadawana ponownie po upływie losowo dobranego czasu według tych samych zasad. Zasadę działania protokołu Aloha ilustruje rys. 4.

Rys. 4. Zasada działania protokołu Aloha
Fig. 4. The rules of Aloha protocol

Odmianą protokołu Aloha jest tzw. Aloha szczelinowa (ang. *Slotted Aloha*) [5, 10]. W protokole tym czas podzielony jest na tzw. szczeliny czasowe (ang. *time slot*). Każda

stacja, po skompletowaniu ramki, musi się wstrzymać z nadawaniem do momentu rozpoczęcia najbliższej szczeliny. Jeżeli więcej niż jedna stacja rozpoczęła nadawanie, oczywiście wystąpi kolizja; jeżeli jednak daną szczelinę wybrała tylko jedna stacja, to ramka ta nie zostanie zniekształcona przez jakąkolwiek inną ramkę. Mechanizm ten podnosi dwukrotnie przepustowość łącza. Zasadę działania tego protokołu ilustruje rys. 5.



Rys. 5. Zasada działania protokołu s-Aloha
Fig. 5. The rules of Slotted-Aloha protocol

3.2. Protokół CSMA/CA

Protokół CSMA/CA (ang. *Carrier Sense Multiple Access with Collision Avoidance*) [10] jest wykorzystywany m. in. w amatorskiej sieci Packet Radio [7, 10]. Po skompletowaniu ramki stacja nadawcza sprawdza stan łącza. Jeśli jest ono wolne, stacja rozpoczyna nadawanie, a jeśli zajęte – transmisja jest wstrzymywana do czasu zwolnienia łącza. W celu wykrycia kolizji lub innych błędów transmisji stacja odbierająca musi wysłać potwierdzenie (pozytywne lub negatywne) odebrania ramki. Ramki przekłamane są nadawane ponownie.

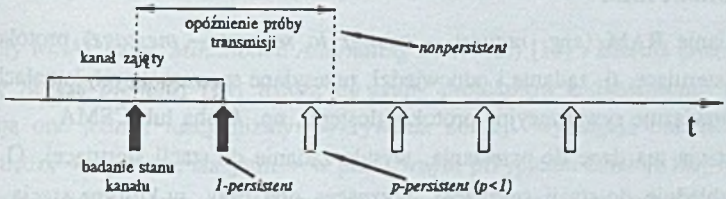
W protokole tym istnieje możliwość kolizji, jeżeli dwie stacje zaczną nadawać równocześnie lub prawie równocześnie po okresie zajętości łącza. Inną możliwą przyczyną kolizji jest opóźnienie propagacyjne, które powoduje błąd oceny stanu łącza (stacja rozpoczyna nadawanie, ponieważ nie odbiera ona jeszcze sygnałów od innej stacji).

Wśród protokołów CSMA wyróżniamy protokoły:

- bez wymuszania transmisji, czyli nietrwałe (ang. *nonpersistent*), w którym stacja, po stwierdzeniu zajętości kanału, losowo dobiera moment następnej próby dostępu;
- z wymuszaniem transmisji z prawdopodobieństwem p, czyli trwałe (ang. *p-persistent*), w którym stacja czeka do chwili zwolnienia kanału, po czym dzieli czas na szczeliny i dokonuje prób transmisji z prawdopodobieństwem p w kolejnych szczelinach; długość szczeliny jest równa podwojonemu maksymalnemu czasowi propagacji w danym kanale.

Niezależnie od wariantu, wysłanie ramki musi być zawsze poprzedzone badaniem stanu kanału. Zasadę działania protokołów CSMA/CA pokazano na rys. 6.

Protokół CSMA/CA z potwierdzaniem odbioru wykorzystywany jest również w niektórych bezprzewodowych sieciach lokalnych. Nie zapobiega on jednak kolizjom, wynikłym z faktu wystąpienia zjawiska ukrytej stacji.



Rys. 6. Zasada działania protokołów CSMA/CA
Fig. 6. The rules of CSMA/CA family protocols

3.3. Protokół BTMA

Protokół BTMA (ang. *Busy Tone Multiple Access*) [3] jest jedną z prób rozwiązania problemu ukrytych stacji. Przyjmuje się, że kanał transmisyjny jest rozbity na dwa podkanały:

- podkanał komunikatów (ang. *message channel*), w którym przesyłane są informacje,
- podkanał zajętości (ang. *busy-tone channel*).

Każda stacja, odbierająca informacje z podkanału komunikatów, wysyła sygnał zajętości (falę sinusoidalną) do podkanału zajętości.

Każda stacja, mająca ramkę do wysłania, sprawdza najpierw stan podkanału zajętości przez pewien czas. Jeżeli sygnał zajętości jest nieobecny, dane są wysyłane; w przeciwnym przypadku natomiast ramka jest odkładana do późniejszego wysłania. Przed ponowną próbą wysłania stacja musi także sprawdzić stan kanału.

Wadą tego protokołu jest konieczność zmniejszenia szerokości kanału transmisyjnego, a więc zmniejszenia maksymalnej prędkości transmisji. Ponadto można łatwo zablokować działanie całej sieci przez stałe wysyłanie sygnału zajętości. Inny problem może wystąpić wskutek różnic w propagacji sygnału w kanale zajętości i kanale danych, ponieważ kanały te wykorzystują różne częstotliwości nośne [11].

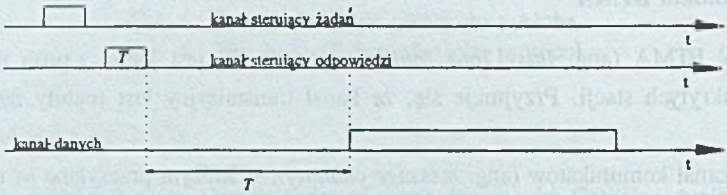
3.4. Protokół SRMA

Protokół SRMA (ang. *Slot Reservation Multiple Access*) [12] wykorzystuje mechanizm dynamicznej rezerwacji przedziałów czasowych, w których dana stacja może nadawać. Przyjmuje się, że, podobnie jak w protokole BTMA, kanał podzielony jest na podkanał komunikatów i podkanał sterujący. Ponadto konieczne jest wprowadzenie do sieci stacji sterującej, której zadaniem jest przydział przedziałów czasowych dla poszczególnych stacji. Kanał sterujący może pracować według wielu reguł. W [12] proponuje się dwa rozwiązania, różniące się zasadami pracy kanału sterującego.

3.4.1. SRMA-RAM

W odmianie RAM (ang. *request – answer to request – message*) protokołu SRMA informacje sterujące, tj. żądania i odpowiedzi, przesyłane są w osobnych kanałach. W kanale żądań obowiązuje rywalizacyjny protokół dostępu, np. Aloha lub CSMA.

Jeżeli stacja ma dane do przesłania, wysyła żądanie do stacji sterującej. O ile żądanie dotarło bezbłędnie do stacji sterującej, wyznacza ona czas, w którym stacja zgłaszająca żądanie może rozpocząć transmisję. Informacja ta jest przekazywana ze stacji sterującej w kanale odpowiedzi, jak pokazano na rys. 7.

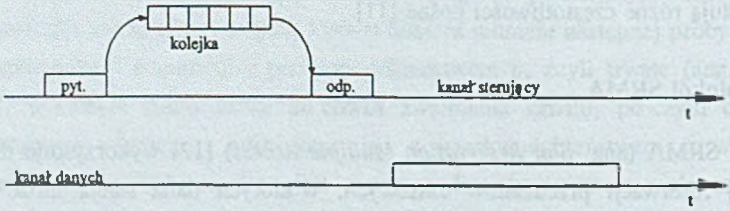


Rys. 7. Zasada działania protokołu SRMA-RAM
Fig. 7. The rules of SRMA-RAM protocol

3.4.2. SRMA-RM

W odmianie RM (ang. *request – message*) kanał sterujący nie jest dzielony na podkanały, tym niemniej obowiązuje w nim także rywalizacyjny protokół dostępu.

Jeżeli stacja ma dane do przesłania, wysyła żądanie do stacji sterującej. Jeśli dotarło ono bezbłędnie, jest dołączane do kolejki żądań. Kolejka ta może być obsługiwana według dowolnego algorytmu. Gdy kanał komunikatów może zostać udostępniony, stacja sterująca przesyła tym kanałem zezwolenie na nadawanie (rys. 8). Jeżeli stacja zgłaszająca żądanie



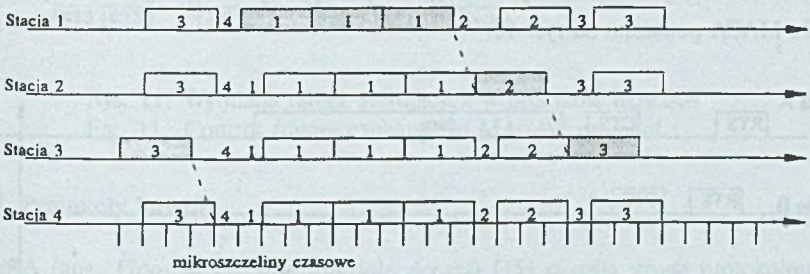
Rys. 8. Zasada działania protokołu SRMA-RM
Fig. 8. The rules of SRMA-RM protocol

nie doczeka się odpowiedzi w określonym czasie, ponawia przesłanie żądania do stacji sterującej.

3.5. Protokoły MSAP i BRAM

Protokoły MSAP (ang. *MiniSlotted Alternating Priorities*) [13] i BRAM (ang. *Broadcast Recognizing Access Method*) [14] należą do grupy protokołów z dynamiczną rezerwacją, wykorzystują one jednak mechanizmy wykrywania nośnej. Wymagają one bezpośredniej łączności między wszystkimi stacjami – w przeciwnym przypadku działają nieprawidłowo.

W protokole MSAP czas podzielony jest na miniszczeliny (ang. *minislot*) o długości równej maksymalnemu czasowi propagacji w sieci. Dostęp do łącza oparty jest na zasadzie kolejno zmiennych priorytetów. Oznacza to, że stacja i, która uzyskała dostęp do łącza, może nadać całą informację, jaką ma do wysłania. Następnie pozostałe stacje wykrywają koniec tej transmisji za pomocą mechanizmu wykrywania nośnej. W tym momencie nadawanie może rozpocząć stacja $(i \bmod N) + 1$, o ile ma ona dane do wysłania. W przeciwnym przypadku transmisję rozpoczyna kolejna stacja. Ideę działania protokołu przedstawiono na rys. 9.



Rys. 9. Idea działania protokołu MSAP
Fig. 9. The idea of MSAP protocol

W protokole MSAP przyjmuje się, że kolejne stacje nie są jawnie wywoływane, ponieważ nie występuje tu centralna stacja sterująca. Każda stacja musi więc liczyć miniszczeliny po każdej transmisji, tak więc protokół jest czuły na błędy wykrywania nośnej.

Protokół BRAM jest w pewnym sensie uogólnieniem protokołu MSAP – wersja priorytetowa (ang. *prioritized BRAM*) jest tożsama z MSAP, czyli umożliwia każdej stacji wysłanie całej informacji w jednym cyklu dostępu do łącza. Przeciwieństwem jej jest wersja sprawiedliwa (ang. *fair BRAM*), w której każda stacja może wysłać co najwyżej jedną ramkę danych w jednym cyklu dostępu.

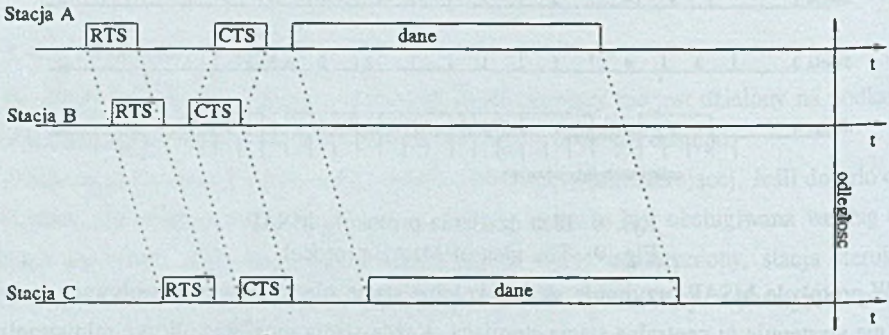
Dla niskich obciążeń sieci, zawierającej dużo stacji, protokół BRAM ma niedużą efektywność, ponieważ liczba miniszczelin, poprzedzających "znalezienie" stacji gotowej do transmisji, jest równa liczbie stacji. Dlatego też korzystne może być podzielenie sieci na grupy stacji. Poszczególne miniszczeliny odpowiadają wówczas grupom, a nie stacjom. W każdej grupie obowiązuje rywalizacja przy dostępie do łącza. Ponieważ liczba grup jest

parametrem sieci, protokół ten nosi nazwę parametryzowanego BRAM (ang. *parametric BRAM*); również i tu wyróżnia się wersję priorytetową i sprawiedliwą.

3.6. Protokoły MACA i MACAW

Analiza zachowania sieci bezprzewodowej zawierającej stacje ukryte bądź odkryte pozwala stwierdzić, że zastosowanie protokołu dostępu do łącza wykorzystującego jedynie śledzenie nośnej jest nieefektywne. W ten sposób powstała propozycja protokołu MACA (ang. *Multiple Access with Collision Avoidance*) [11].

W protokole tym w ogóle nie prowadzi się wykrywania fali nośnej. Transmisja danych poprzedzona jest jednak wymianą informacji sterującej – nadajnik wysyła ramkę RTS, a odbiornik CTS. Mechanizm ten zapobiega występowaniu zjawiska ukrytych i odkrytych stacji. Stacja ukryta odbiera bowiem ramkę CTS odbiornika, stacja odkryta natomiast – ramkę RTS nadajnika. Czas trwania transmisji można łatwo określić, o ile w ramkach sterujących zawarta jest informacja o długości przesyłanej informacji. Zasadę działania protokołu MACA pokazano na rys. 10.



Rys. 10. Zasada działania mechanizmu RTC-CTS w protokole MACA
Fig. 10. The idea of RTS-CTS exchange in MACA protocol

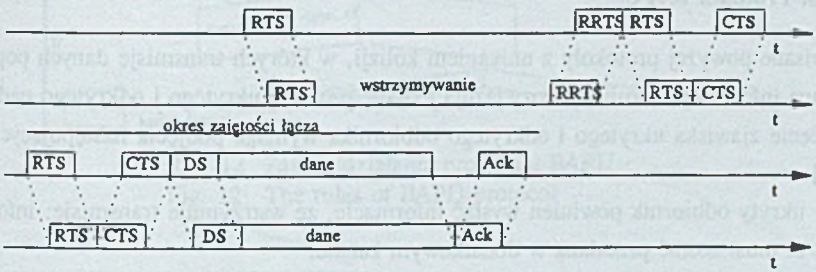
Protokół MACA nie zapobiega jednak wszystkim kolizjom. Istnieje bowiem ryzyko kolizji między ramkami sterującymi. Aby im zapobiec, każda stacja losowo wybiera czas, który musi upłynąć, zanim rozpocznie się transmisja ramki.

Efektywność protokołu w obecności stacji ukrytych i odkrytych przewyższa efektywność protokołu CSMA/CA, pod warunkiem że długość ramek sterujących (RTS i CTS) jest znacznie mniejsza od długości ramek zawierających dane.

Protokół MACAW [2] jest w zasadzie rozwinięciem protokołu MACA, zawierającym szereg uściśleń. Wprowadzono tu m. in. dodatkowe ramki sterujące:

- DS (ang. *Data Sending*), oznaczająca rozpoczęcie nadawania danych; ramka ta informuje pozostałe stacje o pomyślnym zakończeniu negocjacji RTS-CTS;
- Ack (ang. *Acknowledge*), oznaczająca poprawny odbiór ramki danych;
- RRTS (ang. *Request for RTS*), wykorzystywana wówczas, gdy stacja nie może odpowiedzieć na ramkę RTS z powodu wstrzymywania transmisji; po zakończeniu okresu wstrzymywania wysyła ona ramkę RRTS do nadawcy ramki RTS, co umożliwia przeprowadzenie poprawnej negocjacji RTS-CTS.

Zasadę wymiany ramek w protokole MACAW ilustruje rys. 11.



Rys. 11. Wymiana ramek sterujących w protokole MACAW
Fig. 11. Control frames exchange in MACAW protocol

3.7. Protokoły FAMA

FAMA (ang. *Floor Acquisition Multiple Access*) [15] określa grupę protokołów, które stosują wykrywanie nośnej i, znany z protokołów MACA [11] i MACAW [2], mechanizm wymiany ramek sterujących, poprzedzający transmisję danych.

Istotą protokołu FAMA jest dynamiczne zezwalanie poszczególnym stacjom na sterowanie kanałem. Podobne mechanizmy wykorzystywane są w protokołach z dynamiczną rezerwacją (np. SRMA [12], MSAP [13] czy BRAM [14]), jednak FAMA nie wykorzystuje osobnego kanału sterującego ani centralnej stacji sterującej. Przed rozpoczęciem transmisji stacja musi uzyskać kontrolę nad kanałem. Mechanizm przekazywania sterowania odbywa się na zasadzie wymiany informacji sterującej, która jest przesyłana w jednym kanale z danymi w taki sposób, że mimo iż mogą nastąpić kolizje między ramek sterującymi, dane przesyłane są zawsze bez kolizji. Jest to możliwe, jeżeli przestrzegane są określone zależności czasowe, m. in. czas transmisji ramek sterujących nie może być krótszy niż podwojony maksymalny czas propagacji w kanale [15].

W sieciach bezprzewodowych korzystne jest przekazywanie sterowania, oparte na zasadzie wymiany ramek sterujących RTS i CTS ze względu na eliminację zjawiska ukrytych

stacji. W [15] proponuje się wymianę informacji sterującej bądź bez wykrywania nośnej, bądź też z wykrywaniem nośnej bez wymuszania transmisji (ang. *nonpersistent*).

FAMA bez wykrywania nośnej odpowiada protokołowi MACA. Wadą tego protokołu jest możliwość wystąpienia kolizji między danymi a informacją sterującą, spowodowana różnicami w czasie propagacji. Cecha ta nie występuje, jeżeli przed nadaniem ramki sterującej stacja bada stan łącza i wstrzymuje transmisję do czasu jego zwolnienia. Mechanizm ten stosowany jest w protokole FAMA-NTR (ang. *Non-persistent Transmit Request*).

3.8. Protokół BAPU

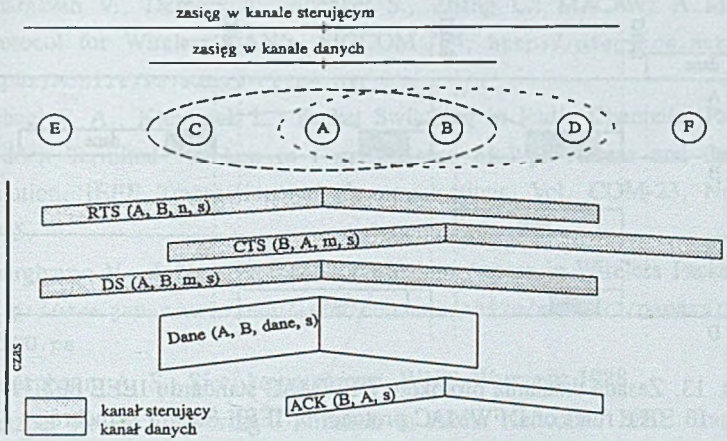
Opisane powyżej protokoły z unikaniem kolizji, w których transmisję danych poprzedza wymiana informacji sterującej, rozwiązują jedynie problem ukrytego i odkrytego nadajnika. Uniknięcie zjawiska ukrytego i odkrytego odbiornika wymaga podjęcia następujących działań [4]:

- ukryty odbiornik powinien wysłać informację, że wstrzymuje transmisję; informacja ta musi zostać przesłana w dodatkowym kanale;
- odkryty odbiornik powinien móc odebrać informację sterującą nawet wtedy, gdy w kanale przebiega inna transmisja danych; warunek ten wymaga rozbicia kanału na kanał danych i kanał sterujący;
- stacje zakłócające powinny być poinformowane o fakcie prowadzenia transmisji; warunek ten można spełnić, zwiększając zasięg informacji sterującej.

Dlatego też w protokole BAPU (ang. *Basic Access Protocol solUtions*) [4] proponuje się wyróżnienie kanału danych i kanału sterującego, przy czym drugi z wymienionych charakteryzuje się większym zasięgiem transmisji. Dzięki takiemu rozwiązaniu stacje, mogące interferować w kanale danych, stają się stacjami ukrytymi bądź odkrytymi w kanale sterującym. W protokole używa się pięciu typów ramek sterujących:

- RTS (ang. *Request To Send*), czyli zgłoszenie gotowości do nadawania,
- CTS (ang. *Clear To Send*), czyli zgłoszenie gotowości do odbioru,
- DS (ang. *Data Sending*), czyli sygnalizacja rozpoczęcia transmisji danych,
- NCTS (ang. *Not Clear To Send*), czyli brak gotowości do odbioru, np. jeżeli stacja jest w zasięgu innej transmisji danych,
- ACK (ang. *Acknowledge*), czyli potwierdzenie porcji danych.

W kanale danych przesyłane są dane i potwierdzenia (ramki ACK), pozostałe ramki są natomiast przesyłane kanałem sterującym. Ideę protokołu wyjaśnia rys. 12 [4].



Rys. 12. Zasada działania protokołu BAPU
Fig. 12. The rules of BAPU protocol

3.9. Protokół standardu IEEE 802.11

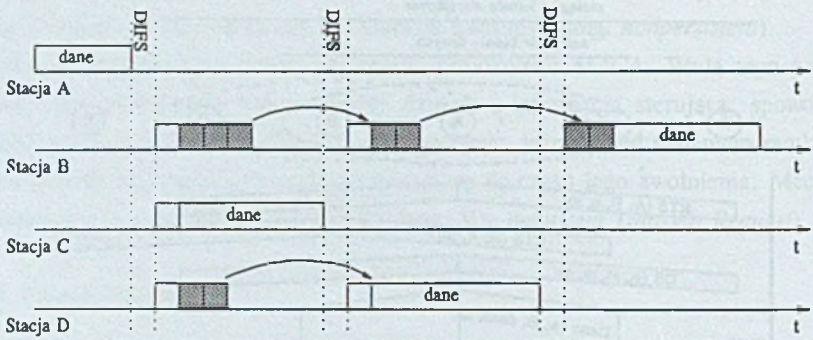
W standardzie IEEE 802.11 [10] zdefiniowano m. in. rywalizacyjny protokół dostępu do łącza DFWMAC (ang. *Distributed Foundation Wireless Medium Access Control*).

Przed rozpoczęciem transmisji stacja sprawdza stan łącza i ewentualnie czeka na zwolnienie kanału przez inne stacje. Następnie czeka jeszcze przez czas DIFS (ang. *Distributed Inter-Frame Space*) i losowo wybiera przedział czasowy, w którym może zacząć nadawać. Transmisja rozpocznie się jednak, pod warunkiem że żadna inna stacja nie wybrała przedziału wcześniejszego. Kolizja może nastąpić zatem jedynie wówczas, gdy więcej stacji rozpoczęło nadawanie w tej samej szczelinie czasowej. Mechanizm ten może zostać uzupełniony o wymianę ramek sterujących RTS i CTS, o ile długość stosowanych ramek danych jest wystarczająco duża, aby było to opłacalne. Zasadę działania protokołu ilustruje rys. 13.

3.10. Protokół standardu HiPeRLAN

W standardzie HiPeRLAN (ang. *High Performance Radio Local Area Network*) [10] określono m. in. zasady rywalizacyjnego dostępu do łącza z uwzględnieniem priorytetów stacji – NPMA (ang. *Non-preemptive Priority Multiple Access*). Na proces uzyskiwania zezwolenia na nadawanie składają się następujące fazy:

- faza zgłaszania priorytetów,
- faza rywalizacji,
- faza transmisji.



Rys. 13. Zasada działania protokołu DFWMAC standardu IEEE 802.11
Fig. 13. The rules of DFWMAC protocol of IEEE 802.11 standard

Szczegółowy opis poszczególnych faz znajduje się w [10].

4. Podsumowanie

W chwili obecnej wydaje się, że jest już rozwiązana większość problemów, występujących podczas stosowania rywalizacyjnych protokołów dostępu do łącza w sieciach bezprzewodowych. Odbywa się to wprawdzie kosztem dużej komplikacji protokołów, jednak narzuty czasowe procedur dostępu do łącza zwracają się w obecności stacji ukrytych i odkrytych.

Na efektywność protokołów wpływają także pewne parametry transmisji, takie jak zasięg i prędkość transmisji, a także długość ramek zawierających dane [15]. Dlatego też interesujące może być zbadanie, jak efektywność protokołu zmienia się w zależności od środowiska pracy sieci bezprzewodowej. Badania takie można przeprowadzić analitycznie (np. [15, 16]), jak również wykorzystując elementy modelowania (np. [2, 4]). Istnieje także możliwość zaimplementowania wybranych protokołów w doświadczalnej sieci bezprzewodowej i dokonania stosownych pomiarów.

LITERATURA

1. Zieliński B.: Bezprzewodowe sieci komputerowe wykorzystujące konwersję protokołów. Rozprawa doktorska, Instytut Informatyki Politechniki Śląskiej, Gliwice 1997.

2. Bhargavan V., Demers A., Shenker S., Zhang L.: MACAW: A Media Access Protocol for Wireless LAN's. SIGCOM '94, http://piggy.cs.nthu.edu.tw/-paper/Mobile/PS/macaw-cr.ps.gz.
3. Tobagi F. A., Kleinrock L.: Packet Switching in Radio Channels: Part II – The Hidden Terminal Problem in Carrier Sense Multiple-Access and the Busy-Tone Solution. IEEE Transactions of Communications, Vol. COM-23, No. 12, Dec. 1975.
4. Bharghavan V.: A New Protocol for Medium Access in Wireless Packet Networks. http://www.janet.ucla.edu/~mbs/courses/1997s/ee298-7/papers/bhargavan-_BAPU.ps.
5. Tannenbaum A. S.: Sieci komputerowe. WNT, Warszawa 1988.
6. Metzner J.: On Improving Utilization in Aloha Networks. IEEE Transactions on Communications, Vol. COM-24, Apr. 1976.
7. Dąbrowski K.: Amatorska komunikacja cyfrowa. PWN, Warszawa 1994.
8. Pahlavan K., Levesque A. H.: Wireless Data Communications. Proceedings of the IEEE, Vol. 82, No. 9, Sept. 1994.
9. Hołubowicz W., Płóciennik P., Różański A.: Systemy łączności bezprzewodowej. Wydawnictwa EFP, Poznań 1996.
10. Nowicki K., Woźniak J.: Sieci LAN, MAN i WAN – protokoły komunikacyjne. Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1998.
11. Karn P.: MACA – A New Channel Access Method for Packet Radio. ARRL Amateur Radio 9 Computer Networking Conference, 22.09.1990. http://people.-qualcomm.com/karn/papers/maca.ps.gz.
12. Tobagi F. A., Kleinrock L.: Packet Switching in Radio Channels: Part III – Polling and (Dynamic) Split-Channel Reservation Multiple Access. IEEE Transactions on Communications, Vol. COM-24, No. 8, Aug. 1976.
13. Kleinrock L., Scholl M. O.: Packet Switching in Radio Channels: New Conflict-Free Multiple Access Schemes. IEEE Transactions on Communications, Vol. COM-28, No. 7, Jul. 1980.
14. Chlamtac I., Franta W. R., Levin K. D.: BRAM: The Broadcast Recognizing Access Method. IEEE Transactions on Communications, Vol. COM-27, No. 8, Aug. 1979.
15. Fullmer C. L., Garcia-Luna-Aceves J. J.: Floor Acquisition Multiple Access (FAMA) for Packet Radio Networks. http://www.janet.ucla.edu/~mbs/courses/-1997s/ee298-7/papers/FAMA_sigcomm95.ps.

16. Kleinrock L., Tobagi F. A.: Packet Switching in Radio Channels: Part I – Carrier Sense Multiple-Access Modes and Their Throughput-Delay Analysis. IEEE Transactions on Communications, Vol. COM-23, No. 12, Dec. 1975.

Recenzent: Dr inż. Leszek Dziczkowski

Wpłynęło do Redakcji 4 marca 1999 r.

Abstract

Wireless networks have different properties than wired ones. There are problems like hidden (Fig. 2) and exposed (Fig. 3) stations, capture effect and interference from out-of-range stations which degrade possibility to sense the collisions. Therefore it is needed to design some new medium access protocols.

There are many random access protocols designed to work with wireless networks, especially radio ones. First of them was Aloha (Fig. 4) and slotted Aloha (Fig. 5), which were very simple but unefficient. Much more efficient is CSMA/CA protocol (Fig. 6), but its efficiency degrades in the presence of hidden and exposed stations. This problem is partially solved in BTMA access scheme.

Another family of protocols are dynamic reservation protocols. Examples are SRMA-RAM and SRMA-RM (Fig. 7 and 8), MSAP and BRAM (Fig. 9). However, their usage requires that no hidden stations exist in the network.

Another way to avoid problem of hidden station is to exchange control packets befor the data transmission, instead of carrier sensing, as in MACA and MACAW protocols (Fig. 10 and 11). These protocols can be viewed as some kind of FAMA protocols family in which station must gain control over the link before it statrs transmission.

The last of presented protocols is BAPU, which solves the problems of hidden and exposed stations as well as interfering stations by using separate control channel of longer range than the data channel. The idea of such a solution is shown on Fig. 12.

The mechanism of control packet exchange before data transmission is also used in the DFWMAC protocol of IEEE 802.11 standard, as shown on Fig. 13.