5 MAC

Bežični komunikacioni sistem, odnosno bežična mreža, se sastoji iz više bežičnih uređaja koji su operativni u određenom ograničenom fizičkom prostoru i pri tom koriste ograničeni segment frekventnog spektra za prenos podataka. U tom kontekstu, bežični medijum, kao kombinacija fizičkog prostora i segmenta frekventnog spektra, predstavlja resurs koji je deljiv, tj. zajednički za sve uređaje u datom bežičnom sistemu. Bežični medijum poseduje dve bitne osobine, koje imaju značajan uticaj na različite aspekte bežične komunikacije:

- Komunikacioni kapacitet bežičnog medijuma (maksimalna količina podataka koja se može preneti u jedinici vremena) je konačan (tj. ograničen), što je određeno brojnim faktorima, poput širine korišćenog frekventnog opsega, uslova propagacije RF signala u konkretnom fizičkom prostoru, efikasnošću antena, izlazne snage predajnika, tipa modulacije itd.
- Bežični medijum je difuzionog karaktera, u smislu da se RF signali ne „vode“ od predajnika do prijemnika već se šire u svim pravcima, što sprečava više prostorno bliskih uređaja da istovremeno emituju svoje RF signale u istom frekventnom opsegu.

Imajući u vidu prethodno, preduslov za pravilno funkcionisanje bežične mreže nameće upotrebu posebnih mehanizama, koji će regulisati raspodelu komunikacionog kapaciteta i koordinisati pristup bežičnom medijumu od strane različitih uređaja (ko, kada, koliko dugo i na koji način može da koristi medijum). Objedinjujući pojam za ove mehanizme je MAC (*Medium Access Control* – kontrola pristupa medijumu). Važno je napomenuti da ne postoji univerzalni set MAC mehanizama, koji se primenjuje u svim mrežama. Umesto toga, postoje brojni tzv. MAC protokoli koji specificiraju načine za rešavanje problema usaglašenog i bezkonfliktnog deljenje bežičnog medijuma, prilagođeni specifičnim zahtevima konkretnih bežičnih mreža, a sve u cilju postizanja efikasne i pouzdane komunikacije. MAC protokoli se svrstavaju u drugi sloj OSI arhitekture (neposredno iznad fizičkog sloja). Po pravilu, implementiraju se u softveru i deo su najnižeg nivoa protokol-steka mrežnih uređaja, koji neposredno upravlja RF primopredajnikom.

Osnovni zadaci MAC protokola su:

- *Deoba* (*zajedničko korišćenje*) *bežičnog medijuma*: Cilj je omogućiti svakom uređaju pristup medijumu u odgovarajućem trenutku.
- *Koordinacija pristupa*: S obzirom na ograničeni komunikacioni kapacitet bežičnog medijuma, MAC protokoli koordiniraju pristup medijumu od strane različitih uređaja, kako bi se izbegli konflikti i osigurala efikasna komunikacija.
- *Razrešavanje konflikata*: Konflikti nastaju kada više uređaja pokušava pristupiti medijumu istovremeno. MAC protokoli implementiraju mehanizme za otkrivanje i razrešavanje ovih konflikata, čime se minimizuje gubitak podataka i poboljšava efikasnost mreže.

MAC protokola može imati i niz sekundarnih zadataka, od kojih su najznačajniji:

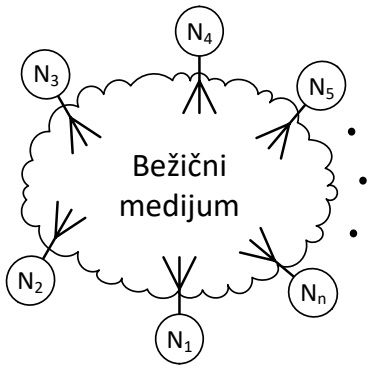
- *Prioriteti i raspodela resursa*: MAC može dodeljivati prioritete različitim vrstama podataka ili uređajima u mreži kako bi se zadovoljile različite potrebe, kao što su prenos podataka u realnom vremenu ili prenos podataka sa višim propusnim opsegom.

- *Sigurnost*: MAC protokoli često uključuju mere sigurnosti kako bi zaštitili komunikaciju od neovlašćenog pristupa ili napada.

MAC protokoli za konvencionalne bežične mreže (poput WiFi) teže balansu između propusnosti, kašnjenja i pravičnosti. Kod MAC protokola za bežične mreže u embeded i IoT domenu, naglasak je često na energetskoj efikasnosti. Odnosno, balans se traži između energetske efikasnosti s jedne i tradicionalnih mera komunikacionih performansi (propusnost, kašnjenje, pravičnost) s druge strane.

5.1 Klasifikacija MAC protokola

Na Sl. 1 je prikazan opšti model problema višestrukog pristupa (*multiple-access*). Pretpostavka je da se komunikacija obavlja u okviru određenog frekventnog opsega koji je eventualno podeljen na više frekventnih kanala. Takođe, informacija koju u medijum emituje bilo koji uređaj može biti primljena od strane svih drugih uređaja u okolini. Stoga, ako više od jednog uređaja istovremeno emituje na istom kanalu, dolazi do mešanja emitovanih RF signala i gubitka poslatih informacija. Ova pojava se naziva *kolizija* ili problem višestrukog pristupa (*multiple-access*). Kolizije, naravno, treba izbeći, a to se postiže praćenjem pravila komunikacije koja su definisana određenim MAC protokolom. Cilj primene ovih pravila je da se odredi koji uređaj ima pravo ekskluzivnog pristupa frekventnom kanalu u datom trenutku, ili tokom određenog vremena, kako bi taj uređaj mogao da prenese, a drugi uređaji da prime, razumeju i tumače poslate informacije.



Sl. 1 Problem višestrukog pristupa

Za rešavanje problema višestrukog pristupa primenjuju se dva generalna metoda:

Statička alokacija resursa, gde su resursi bežičnog medijuma fiksno raspodeljeni među svim uređajima (u vremenskom, frekventnom ili kodnom domenu) i ova raspodela se ne menja tokom vremena (ili se ne menja u nekom dužem vremenskom periodu).

Dinamička kontrola pristupa medijumu, gde se medijum dodeljuje uređaju na zahtev (onda kad mu je potreban). Dinamička kontrola pristupa medijumu se postiže:

Planiranje resursa (*schedule-based*), podrazumeva da uređaj, na neki način, od nekoga, traži pristup medijum, i da taj neko, na osnovu prispelih zahteva, pravi plan raspodele resursa i shodno tom planu uređajima dodeljuje vreme, frekvenciju ili kôd na privremeno korišćenje. Ovaj pristup zahteva podršku centralnog entiteta koji bi se bavio planiranjem i raspodelom resursa, što je najčešće uloga centralnog čvora ili koordinatora mreže. U okviru ovog poglavlja, nećemo dalje razmatrati MAC protokole iz ove kategorije. Ipak, pojedini mrežni standardi, od kojih će neki biti obrađeni u narednim poglavljima, koriste i ovaj pristup.

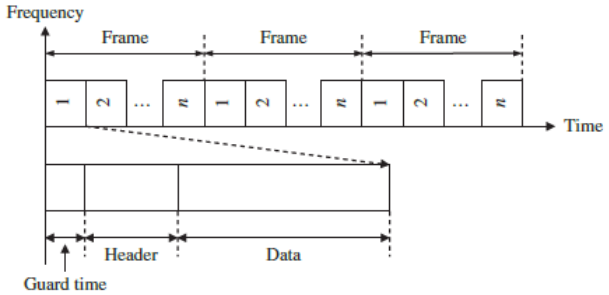
Slučajni pristup (*random access*), omogućava mrežnom uređaju da bez prethodne koordinacije pristupa medijumu uvek kada ima potrebu za tim, ali uz obavezu da se pre samog emitovanja izbori sa drugim uređajima za pravo pristupa. Za razliku od prethodnog, ovaj pristup ne zahteva centralni entitet, već se u potpunosti realizuje kroz funkcionalnost mrežnih uređaja.

5.2 MAC protokoli sa statičkom alokacijom

Kod MAC protokola sa statičkom alokacijom resursa, raspoloživi resursi bežičnog medijuma se dele među čvorovima na duži vremenski period (reda minuta, sati, ili duže) tokom kojeg svaki uređaj ima ekskluzivno pravo na deo resursa koji mu je dodeljen, bez straha od kolizije. Uređaji ne moraju da primenjuju nikakve mere zaštite od kolizija, niti da gube vreme i dodatne resurse radi nadmetanja sa drugim uređajima. Međutim, kod primene ovih protokola nastaje problem kada se promeni topologija mreže, recimo zbog isključenja uređaja, dodavanja novog uređaja ili premeštanja uređaja na drugu lokaciju. Za takve situacije, potreban je neki mehanizam za signalizaciju da bi se izvršila preraspodela resursa, što dovodi u pitanje skalabilnost ovih protokola. Tipični predstavnici klase protokola sa statičkom alokacijom su protokoli poznati pod skraćenicama: TDMA, FDMA i CDMA.

5.2.1 TDMA

TDMA (*Time Division Multiple Access*) - podeli podleže vreme, koje se deli na cikluse fiksnog trajanja (tzv. frejmove, ili vremenske okvire), a svaki frejm na vremenske slotove. Slotovi se dodeljuju mrežnim uređajima na ekskluzivno korišćenje, tako da svaki uređaj može da šalje svoje podatke samo za vreme trajanja svog slota, što se dešava periodično, tj. jedanput tokom svakog frejma (Sl. 2).



Sl. 2 TDMA: vreme je podeljeno na frejmove, a frejmovi na slotove; slot počinje zaštitnim kašnjenjem (*guard time*); trajanje slota je dovoljno za prenos paketa maksimalne dužine

Neke od prednosti TDMA šeme su sledeće:

- *Garantovana propusnost*: Fiksna podela vremena znači da je svakom uređaju dodeljen jedan fiksni deo ukupnog komunikacionog kapaciteta bežičnog kanala. Na taj način, svaki čvor ima na raspolaganju garantovanu propusnost za prenos svojih podataka. Pri tom, postoji mogućnost da čvorovi sa većim zahtevima dobiju ne jedan, već više slotova u frejmu. Uz to, TDMA se može prilagoditi tako da podržava uređaje sa različitim brzinama prenosa podataka.
- *Velika brzina prenosa podataka*: u okviru svog slota, uređaj ima na raspolaganju celokupan frekventni opseg koji je dodeljen bežičnoj mreži, a ne samo jedan uži frekventni kanal (što je slučaj kod FDMA). Širi frekventni opseg znači i mogućnost prenosa podataka većom brzinom.
- *Predvidljivost komunikacije*. Komunikacija u TDMA mreži je predvidljiva, jer se tačno zna u kom trenutku emituje svaki uređaj.

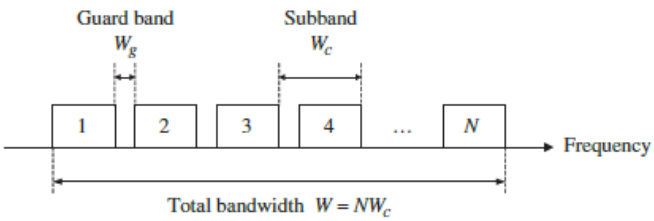
- *Smanjena interferencija*. Budući da bežični uređaji dele vreme, a ne frekvenciju, smanjuje se mogućnost interferencije istovremenih transmisija različitih uređaja.
- *Energetska efikasnost*. Osnovna postavka TDMA je da uređaj emituje samo u svom slotu. Šta radi u ostalim slotovima? Jedna mogućnost je da vreme u ostalim slotovima provodi na prijemu, uvek spreman da primi podatke koje će mu neko poslati. Međutim, u razuđenim mrežama, poput rešetke, gde nisu svi uređaji jedan drugom u radio dometu, uređaj može da isključi svoj RF transiver u slotovima koji ne pripadaju njegovim neposrednim susedima. Odnosno, uređaj emituje u svom slotu, na prijemu je u slotovima svojih suseda, dok vreme u preostalim slotovima provodi u režimu mirovanja (spavanja), odnosno štedi energiju.

Međutim, TDMA ispoljava i izvesne nedostatke:

- *Sinhronizacija*. TDMA nameće potrebu za preciznom vremenskom sinhronizacijom uređaja, da bi se izbeglo preklapanje slotova dodeljenih susednim uređajima. S obzirom da uređaji u mreži prate protok vremena svojim lokalnim časovnicima, koji nisu idealno tačni i precizni, izvesna vremenska neusaglašenost između uređaja je neizbežna. Da bi se kompenzovala ova neusaglašenost, uređaj ne počinje emitovanje na samom početku svog slota, već tek nakon isteka tzv. zaštitnog kašnjenja (*guard time*). Na ovaj način se izbegava preklapanje emitovanja u susednim slotovima. Trajanje slota je obično tako izabrano da omogući prenos jednog paketa maksimalne dužine, što uključuje zaglavlje paketa i podatke. Trajanje zaštitnog kašnjenja zavisi od nivoa ostvarene vremenske sinhronizacije. Na primer, u mreži zvezdaste topologije, relativno je lako ostvariti preciznu sinhronizaciju između centralnog i perifernih čvorova, što omogućava kraće zaštitno kašnjenje. S druge strane, u mrežama topologije stabla, a posebno rešetke, preciznu vremensku sinhronizaciju na nivou cele mreže je daleko teže postići, što se onda mora kompenzovati dužim zaštitnim kašnjenjem.
- *Neracionalno korišćenje komunikacionog kapaciteta*. U slučajevima kada uređaj ne koristi svoj dodeljeni vremenski slot, taj deo vremena ostaje neiskorišćen, odnosno, ne može se dodeliti nekom drugom uređaju, koji trenutno ima povećanu potrebu za komunikacijom.
- *Velika latencija*. TDMA uređaj mora da sačeka svoj slot da bi počeo emitovanje. To znači da vreme prenosa poruke ne uključuje samo vreme koje je potrebno za emitovanje poruke, već i vreme čekanja na početak slota. U proseku, ovo vreme čekanja jednako je polovini trajanja frejma, što može biti prilično dug interval.
- *Slabije performanse sa povećanim brojem korisnika* (uređaja). Sa povećanjem broja umreženih uređaja, efikasnost TDMA može opasti, jer se mora povećati broj vremenskih slotova. Veći broj slotova u frejmu povlači i veće režijske troškove (*overhead*). Razlog za to je što se deo svakog slota mora rezervisati za zaštitno kašnjenje i prenos zaglavlja paketa. Što je broj slotova u frejmu veći to će i *overhead*-i ovog tipa biti veći, odnosno, za prenos podataka će ostati manji deo ukupnog vremena.

5.2.2 FDMA

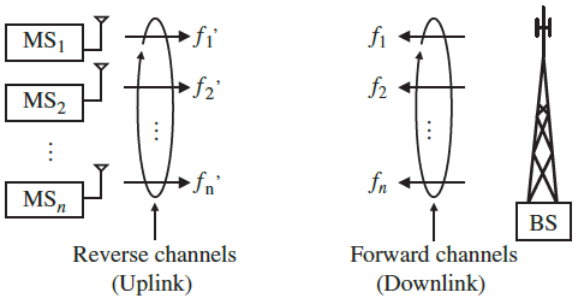
FDMA (*Frequency Division Multiple Access*) - raspoloživ frekventni opseg se deli na podopsege (frekventne kanale) koji se dodeljuju uređajima, tako da svaki uređaj dobija frekvenciju na kojoj ima ekskluzivno pravo emitovanja. Dodela je fiksna i uređaji zadržavaju dodeljen frekventne kanale tokom vremena. Princip je ilustrovan na Sl. 3. Slično zaštitnom kašnjenju kod TDMA, susedni frekventni kanali su razdvojeni zaštitnim opsegom (*guard band*), kako bi se minimizirala interferencija između njih. Noseća frekvencija kanala je obično po sredini opsega dodeljenog kanalu i spektar signala bi samo u minimalnom obimu trebalo da prelazi u zaštitni opseg.



Sl. 3 FDMA: Frekventni opseg širine NW_c je podeljen na N frekventnih kanala širine W, od kojih svaki obuhvata i zaštitni opseg (*guard band*) širine W_g

Tipičan primer FDMA je u analognim radio-difuznim mrežama, gde različite radio stanice koriste različite frekventne kanale. FDMA se takođe koristi i u mrežama za digitalni prenos podataka, kao npr. u celularnoj mreži (Sl. 4). U ovom slučaju, za komunikaciju između svakog mobilnog uređaja i baze stanice koriste se dva frekventna kanala, jedan na kome uređaj emituje dok bazna stanica prima podatke (*uplink*), i drugi za komunikaciju u suprotnom smeru (*downlink*). Ovaj primer ukazuje na glavne prednosti FDMA:

- FDMA, poput TDMA, eliminiše kako direktne kolizije između čvorova tako i njihovu međusobnu interferenciju. Prednost FDMA u odnosu na TDMA je manje kašnjenje u prenosu podataka, jer čvor ne mora da čeka na svoj slot da bi počeo prenos. Suprotno tome, čvor može da emituje svoje podatke „kad god poželi“.
- U vezi s prethodnim je i jednostavnija implementacija FDMA u odnosu na TDMA, jer čvor (mobilni uređaj) ne mora da vodi računa o protoku vremena i striktnoj vremenskoj sinhronizaciji; dovoljno je da podesi svoj predajnik na frekvenciju dodeljenog kanala. Međutim, smanjena složenost uređaja se ovde postiže na račun veće složenosti bazne stanice, koja mora biti u mogućnosti da istovremeno prima/emituje na različitim frekventnim kanalima.



Sl. 4 FDMA u celularnoj mreži

Potrebno je napomenuti da se podela frekventnog opsega na kanale takođe sreće i kod većine WPAN i WLAN mreža, ali sa drugačijom svrhom nego u FDMA celularnoj mreži. Naime, umesto da se pojedinačni kanali dodeljuju uređajima, celokupna mreža (svi uređaji u mreži) rade na istom kanalu, koji se bira na način da se minimizuje interferencija sa drugim mrežama i sistemima u okolini koji koriste taj isti frekventni opseg.

Nedostaci:

- Rad na više frekvencija podrazumeva preciznu frekventnu sinhronizaciju, upotrebu selektivnih uskopojasnih filtera i RF primopredajnika koji imaju sposobnost biranja frekvencije emitovanja/prijema, što ih čini skupljim od onih koji rade u TDMA režimu.
- Ostali nedostaci FDMA su, uglavnom, isti oni od kojih pati i TDMA: *a*) otežano dodavanje novih korisnika ili uređaja bez promene tekuće alokacije frekventnih kanala, *b*) pad komunikacionog

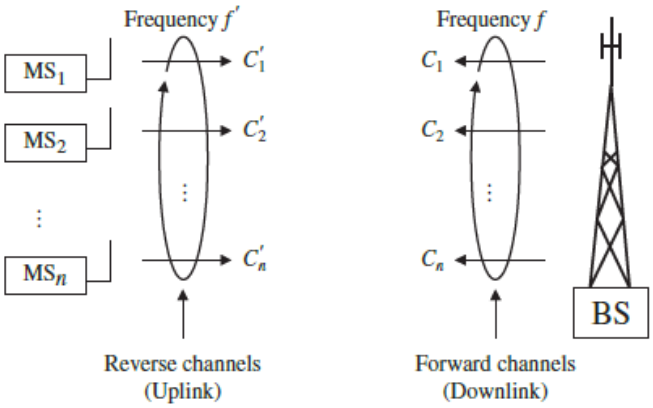
kapaciteta sistema sa povećanjem broja korisnika, i *c*) dodeljeni frekventni kanali su zauzeti i kada nema aktivne komunikacije, što može rezultirati neefikasnim korišćenjem resursa. Za razliku od TDMA gde uređaju može relativno lako da se dodeli više vremenskih slotova, kod FDMA mogućnost dodele više frekventnih kanala istom uređaju može značajno povećati složenost sistema.

5.2.3 CDMA

CDMA (*Code Division Multiple Access*) – je tehnika pristupa medijumu koja omogućava bežičnim uređajima da koriste isti frekventni opseg istovremeno, ali koristeći različite *kôdne sekvence*. Naime, na predajnoj strani, pre emitovanja, izvorna bit-sekvenca se „množi“ pseudo-slučajnom bit-sekvencom značajno veće frekvencije (kôd), čijim se emitovanjem zauzima značajno širi propusni opseg nego što je to neophodno. Prednost CDMA šeme je ta što se korišćenjem različitih CDMA kôdova mogu ostvariti istovremeni prenos bez kolizija - da bi povratio izvorni podatak prijemnik mora da zna kôd koji je predajnik koristio; pri tom svi ostali prenosi, koji koriste različite kôdove, deluju kao šum. Zapravo, na prijemu, izvorni podatak se regeneriše množenjem primljenog signala odgovarajućom kôdnom sekvencom. U suštini, ovde se kôdovi koriste za razdvajanje signala emitovanih od strane različitih uređaja, čime se sprečavaju kolizije i smanjuje međusobna interferencija.

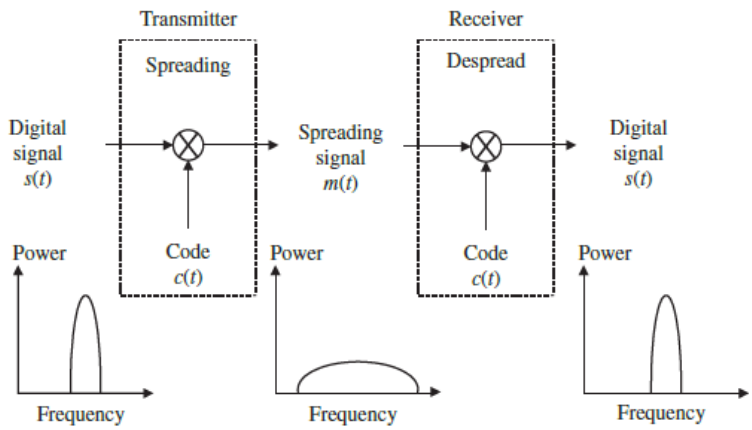
Na Sl. 5 je ilustrovana struktura CDMA sistema na primeru celularne mreže. Svi mobilni uređaji emituju svoje signale u istom frekventnom opsegu, ali korišćenjem različitih kôdova. Za komunikaciju u suprotnom smeru, od bazne stanice ka mobilnim uređajima, koristi se neki drugi frekventni opseg, s tim što su signali kodirani posebnim kôdom za svaki mobilni uređaj.

Treba obratiti pažnju na to da se kod CDMA koristi **celokupan** frekventni opseg, a ne samo jedan frekventni kanal, kao što je to slučaj kod FDMA.



Sl. 5 CDMA na primeru celularne mreže

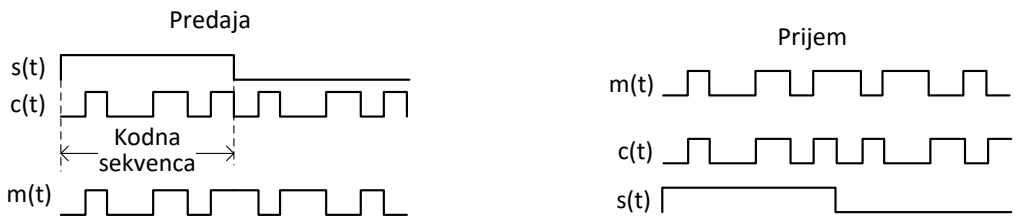
CDMA sistemi se oslanjaju na tehniku prenosa podataka koja je poznata pod nazivom *prošireni spektar* (*spread spectrum*), gde modulisani signal zauzima veći propusni opseg nego što je to neophodno. Proširenje spektra (propusnog opsega emitovanog signala) se postiže upotrebom kôda koji je nezavisan od podataka koji se prenose. Isti kôd se koristi i za demodulaciju podataka na prijemnoj strani. Princip je ilustrovan na Sl. 6. Signal $s(t)$, tj. informacija koja se šalje, množi se kôdnim signalom $c(t)$ veće učestanosti. Na taj način se formira signal, $m(t)$, koji se emituje: $m(t) = s(t) \otimes c(t)$. Spektar signala $m(t)$ je značajno širi od spektra izvornog signala $s(t)$. Ključna osobina operatora $\otimes$ je da važi $s(t) = m(t) \otimes c(t)$, što na prijemnoj strani omogućava demodulaciju (ekstrakciju) izvorne informacije iz primljenog signala, pod uslovom da je prijemniku poznat kôd $c(t)$ koji je korišćen na predajnoj strani. Postoje dva oblika proširenja spektra: *a*) direktna sekvenca (DS - *direct sequence*) i *b*) frekventno skakanje (FH – *frequency hopping*).



Sl. 6 Princip širenja spektra

5.2.3.1 Direktna sekvenca

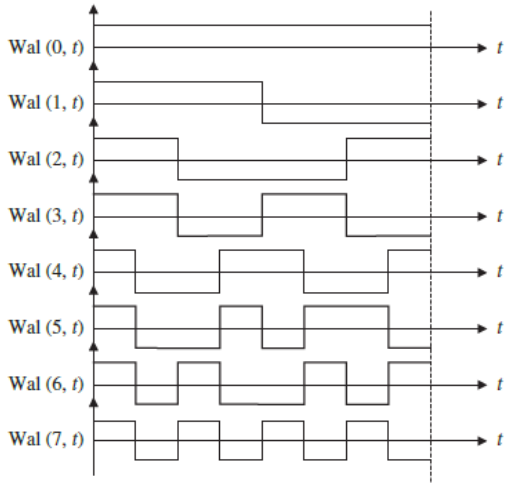
Proširenje spektra direktnom sekvencom (DSSS – *direct sequence spread spectrum*) podrazumeva da se izvorni signal množi pseudo-slučajnom sekvencom čija je frekvencija, pa time i propusni opseg, značajno širi u odnosu na izvorni signal. Tipično, kao operator množenja, ovde se koristi logička operacija XNOR. Kao što vidimo na Sl. 7(a), izvorni podatak, $s(t)$, je dužine dva bita „10“. Za proširenje spektra se koristi kôdna sekvenca dužine 8 bita, „01001101“. Uobičajeno, za kôdnu sekvencu se koristi pojam čip-sekvenca, a za svaki njen bit pojam čip. Na predajnoj strani, između izvornog podataka i čip-sekvence primenjuje se XNOR operacija. Rezultujući signal, $m(t)$ je identičan čip sekvenci ako je vrednost bita podatka 1. U suprotnom ako je bit podatke jednak 0, signal $m(t)$ je po obliku, identičan komplementu čip-sekvence. Na prijemnoj strani, signal $m(t)$ se množi čip-sekvencom, tj. primenjuje se operacija XNOR između $m(t)$ i $c(t)$, kao na Sl. 7(b). Rezultat ovog množenja je izvorni podatak $s(t)$. (Kao što znamo, za operaciju XNOR važi: $(x \otimes y) \otimes y = x$.)



Sl. 7 Princip direktne sekvence

Da bi se u CDMA sistemu omogućilo istovremeno emitovanje signala više predajnika, svakom uređaju se dodeljuje jedinstvena kodna sekvencu. Međutim, dodela jedinstvenih kodova nije dovoljna. Dodatni uslov koji mora biti ispunjen jeste da su ovi kodovi *ortogonalni*. Jedna važna klasa ortogonalnih kodova u CDMA sistemima su tzv. Volšovi kôdovi (*Walsh codes*). Na primer, na Sl. 8 su prikazane sekvence 8-bitnog Volšovog koda u obliku digitalnih signala. Sekvenca 0 sadrži 8 jedinica, sekvenca 1 počinje sa 4 jedinice i završava se sa 4 vrednosti -1, i tako dalje. Poslednja sekvenca, sekvenca 7, sadrži naizmenični niz vrednosti 1 i -1. Ono što čini ovaj skup sekvenci ortogonalnim je osobina da je kros-korelacija između bilo koje dve sekvence jednaka nuli. Kros-korelacija se izračunava množenjem dve sekvence i aritmetičkim sabiranjem rezultujućih vrednosti. Na primer, proizvod sekvenci 0 i 1 rezultira nizom (1,1,1,1,-1,-1,-1,-1), što se sabira do 0. Proizvod između sekvence 3 (1,1,-1,-1,1,1,-1,-1) i sekvence 5 (1,-1,-1,1,-1,1,1,-1) daje sekvencu (1,-1,1,-1,-1,1,-1,1), koja se takođe sabira do 0. Volšove sekvence se generišu iterativnim postupkom konstrukcije tzv. Hadamard-ove matrice, polazeći od početne matrice $H_0 = [0]$, a zatim iterativno primenjujući sledeću formulu:

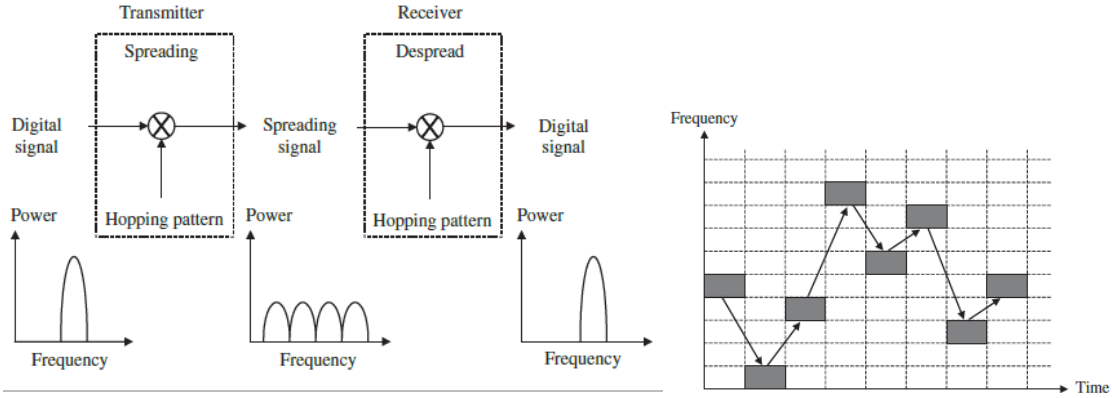
$$H_n = \begin{pmatrix} H_{n-1} & H_{n-1} \\ H_{n-1} & \overline{H_{n-1}} \end{pmatrix}.$$



Sl. 8 8-bitne Volšove sekvence

5.2.3.2 Frekventno skakanje

Proširenje spektra frekventnim skakanjem (FHSS – *Frequency hopping spread spectrum*) podrazumeva upotrebu pseudo-slučajne sekvence za promenu frekvencije signala koji se emituje, odnosno za promenu frekventnog kanala. U ovom slučaju, kodna sekvenca je niz celih brojeva (poput 0,3,4,6,2,1,5,7) gde svaki broj u sekvenci predstavlja redni broj frekventnog kanala iz jednog šireg frekventnog opsega. Frekvencija emitovanja se menja u skladu sa kodnom sekvencom. Na primer, određeni deo vremena, emitovanje se vrši na frekventnom kanalu 0, zatim na kanalu 3, potom na kanalu 4 itd. Na ovaj način, spektar rezultujućeg kanala je proširen na kompletan frekventni opseg. Da bi prijemnik ispravno primio poslatu informaciju, on mora, u sinhronizmu sa predajnikom, da menja prijemnu frekvenciju shodno kodnoj sekvenci.



Sl. 9 Princip frekventnog skakanja. Operator „X“ ovde znači izbor frekvencije predaje/prijema. „*Hopping sequence*“ – sekvenca skakanja

Razlikuju se dve metode frekventnog skakanja: brzo i sporo. Kod brzog skakanja, frekvencija emitovanja se menja više puta tokom svakog bit-intervala. Kod sporog, emitovanje na istoj frekvenciji obuhvata više bit-intervala. Na Sl. 9 je ilustrovan koncept frekventnog skakanja. Redosled promene frekventnih kanala je određen kodnom sekvencom. Predajnik ostaje na istoj frekvenciji fiksno vreme, a onda prelaze na sledeću frekvenciju određenu kodnom sekvencom. Ako je ovo vreme manje od bit-intervala, reč je o brzom, a ako je veće, o sporom frekventnom skakanju. Frekventno skakanje

omogućava da se bežični medijum istovremeno koristi za više emisija, sve dok predajnici koriste različite kodne sekvence, koje se uz to ni ne sudaraju (tj. ni u jednom vremenskom intervalu dva predajnika ne emituju na istoj frekvenciji). Za ovakve kodne sekvence se kaže da su ortogonalne.

Proširenje spektra frekventnim skakanjem se primenjuje kod pojedinih WPAN mreža i to u varijanti sporog skakanja. Naime, predajnik emituje celokupni paket jednoj frekvenciji, a zatim, za prenos sledećeg paketa bira sledeći kanal iz sekvence skakanja. Motiv za frekventno skakanje je izbegavanje interferencije sa drugim mrežama u okolini.

Osim TDMA, FDMA i CDMA, postoje i MAC protokoli zasnovani na kombinovanju različitih načina podele. Recimo, moguće je koristiti TDMA šemu za podelu vremena na slotove, a FDMA (ili CDMA) za razdvajanje transmisija u okviru slota.

5.3 MAC protokoli sa nadmetanjem

Dinamička kontrola pristupa medijumu ostvaruje se upotrebom MAC protokola sa nadmetanjem (*contention-based MAC*). Kod ovih protokola ne postoji fiksna raspodela resursa već se uređaji međusobno nadmeću (takmiče) da bi se izborili za pravo pristupa zajedničkom bežičnog medijuma. Ovo takmičenje za pristup može biti: *a*) implicitno, u smislu da se oslanja na strategiju slučajnog pristupa (*random access protocols*), kada uređaji nasumično biraju vreme slanja svojih podataka ili *b*) eksplicitno, gde uređaji prolaze kroz čitavu proceduru međusobnog nadmetanja i samo pobednik u ovom nadmetanju stiče pravo da pošalje svoje podatke (*collision resolution protocols*). Mehanizmi za nadmetanje nisu idealni, u smislu da mogućnost kolizije nije u potpunosti isključena, uprkos tome što su uređaji, tokom nadmetanja, uradili sve šta se od njih očekivalo. Zbog toga, protokoli iz ove kategorije obično uključuju i mehanizme za detekciju i razrešavanje kolizija. MAC protokoli sa nadmetanjem su efikasni u uslovima promenljivog opterećenja u mreži, npr. onda kada su uređaji veći deo vremena neaktivni, a tek povremeno imaju potrebu za komunikacijom. Međutim, MAC protokoli sa nadmetanjem gube na efikasnosti u uslovima velike zauzetosti bežičnog medijuma (zbog porasta stope kolizija). U nastavku će biti predstavljeno nekoliko MAC protokola iz ove kategorije.

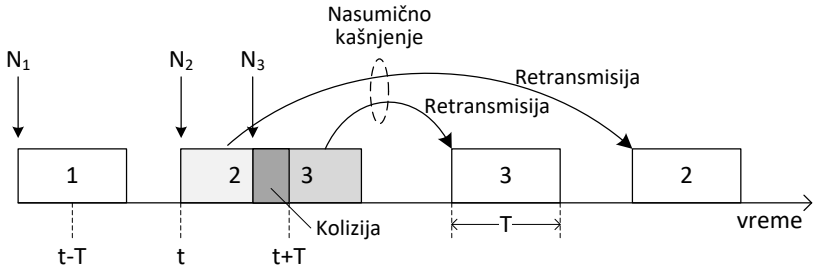
5.3.1 ALOHA

Istorijski posmatrano, prvi, ali i dalje izuzetno značajan protokol iz ove grupe je ALOHA (kaže se i *čista ALOHA – Pure ALOHA*). Razvijen je sedamdesetih godina prošlog veka na Univerzitetu Havaji. Ovaj protokol je dizajniran za primenu u bežičnim mrežama zvezdaste topologije, koja obuhvata jedan centralni i proizvoljan broj perifernih uređaja. Ključna pretpostavka ovog protokola jeste da periferni uređaji komuniciraju isključivo sa centralnim uređajem, a ne međusobno. Princip rada ALOHA protokola je izuzetno jednostavan: uređaj koji želi da pošalje paket to čini odmah, bez odlaganja, bez obzira na mogućnost kolizije. Nakon uspešnog prijema paketa, centralni uređaj šalje odmah potvrdu prijema pošiljaocu. Ukoliko se paket ne potvrdi, predajni uređaj pretpostavlja da je došlo do kolizije. Tada se povlači na nasumično odabrano vreme pre nego što ponovo pošalje (retransmituje) isti paket.

Rad protokola ALOHA je ilustrovan na Sl. 10. Strelice na ovoj slici označavaju trenutke generisanja paketa (tj. trenutke kada je uređaj "oseti potrebu" da pošalje paket). Uspešni prenosi označeni su belim pravougaonicima, dok sivi pravougaonici predstavljaju pakete koji su pogođeni kolizijom. Primetimo trenutak t na Sl. 10 kada uređaj N_2 započinje slanje svog paketa "2". Ovaj paket će biti uspešno prenet ukoliko u bežičnoj mreži ne postoji ni jedan drugi uređaj koji je počeo prenos svog paketa u vremenskom intervalu $t - T$ i $t + T$, gde je T vreme prenosa (emitovanja) paketa (uz pretpostavku da prenos svih paketa traje isto vreme, T). Vremenski interval $[t - T, t + T]$ predstavlja "period ranjivosti" paketa „2“ i njegovo trajanje iznosi $2T$. U primeru na Sl. 10, uređaj N_3 počinje

emitovanje svog paketa "3" pre isteka perioda ranjivosti za paket "2", što dovodi do kolizije. Oba paketa, "2" i "3", su uništena, centralni uređaj ne prima nijedan paket i ne odgovara potvrdama. Pošto nisu primili potvrdu za poslati paket, uređaji N_2 i N_3 zaključuju da je došlo do kolizije i ponavljaju slanje istih paketa, ali ne odmah, već tek nakon nasumično odabranog kašnjenja. S obzirom da uređaji N_2 i N_3 nasumično biraju iznos retransmisionog kašnjenja, postoji šansa da prilikom ponovljenog slanja neće doći do kolizije.

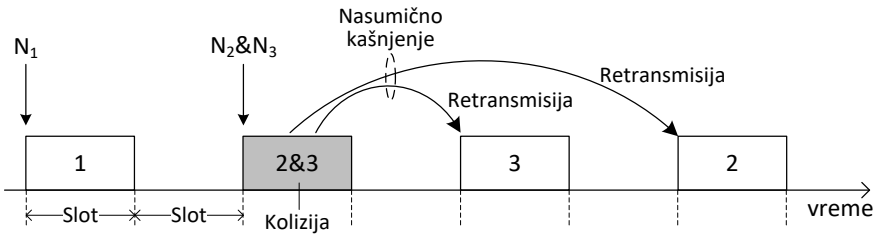
Uočimo, takođe, da Sl. 10 ilustruje pojavu *delimične* kolizije, koja nastaje preklapanjem kraja emitovanja paketa „2“ i početka emitovanja paketa „3“. Bez obzira što kolizijom nisu pogođeni kompletni paketi (što bi prestavljalo *potpunu* koliziju), primljena informacija je neupotrebljiva za centralni uređaj, jer greška na samo jednom bitu paketa dovodi do odbacivanja kompletnog paketa.



Sl. 10 „Čista“ ALOHA

Slotted ALOHA

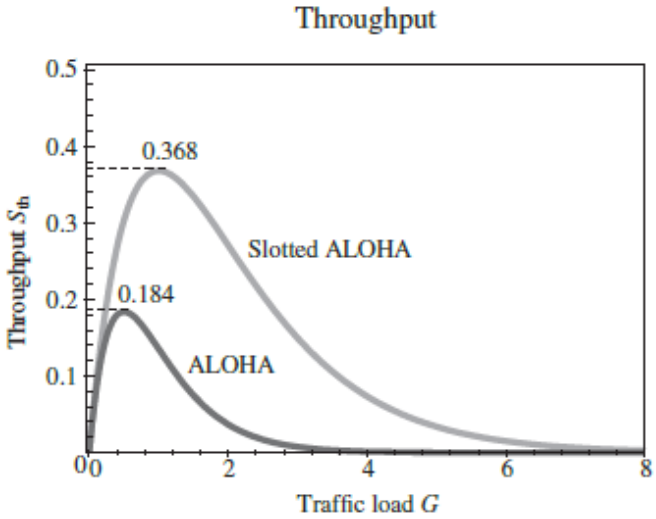
Protokol *Slotted* ALOHA predstavlja modifikaciju originalnog, *Pure* ALOHA protokola, koja se sastoji u podeli vremena na vremenske slotove, sa dužinom slota jednakom trajanju prenosa jednog paketa. Sada, uređaj ne počinje emitovanje paketa istog trenutka kada je paket kreiran. Umesto toga, ako uređaj ima paket za slanje, čeka početak prvog sledećeg slota pre slanja. *Slotted* ALOHA predstavlja poboljšanje u odnosu na *Pure* ALOHA jer smanjuje period ranjivosti paketa na jedan slot. To znači da će prenos biti uspešan samo ako je tačno jedan paket planiran za prenos u trenutnom slotu. Drugim rečima, period ranjivosti je jednak trajanju slota, T, i duplo je kraći od perioda ranjivosti kod *Pure* ALOHA, gde iznosi, $2T$. Na Sl. 11 je prikazan mehanizam kolizija kod *Slotted* ALOHA protokola. Uočimo da su sada, za razliku od *Pure* ALOHA, sudari paketa potpuni.



Sl. 11 *Slotted* ALOHA

Na Sl. 12 je prikazan grafikon propusnosti *Pure* ALOHA i *Slotted* ALOHA protokola u zavisnosti od parametra G (ponuđeni saobraćaj – *Traffic load*). Ponuđeni saobraćaj se odnosi na brzinu generisanja paketa, izraženu prosečnim brojem paketa koji se generiše u celokupnoj mreži u vremenu prenosa jednog paketa, T. Na primer, $G = 2$ znači da se u celokupnoj mreži, koja obuhvata proizvoljan broj mrežnih uređaja, na svakih T sekundi generišu dva paket. Propusnost (*throughput*) je izražena kao deo komunikacionog kapaciteta bežične mreže koji je iskorišćen za uspešne prenose paketa, odnosno koliko paketa primi centralni uređaj tokom vremena T. Na primer, propusnost 1 bi značila da je celokupno vreme ispunjeno uspešnim prenosima paketa i da se kolizije nikada ne dešavaju, što je u

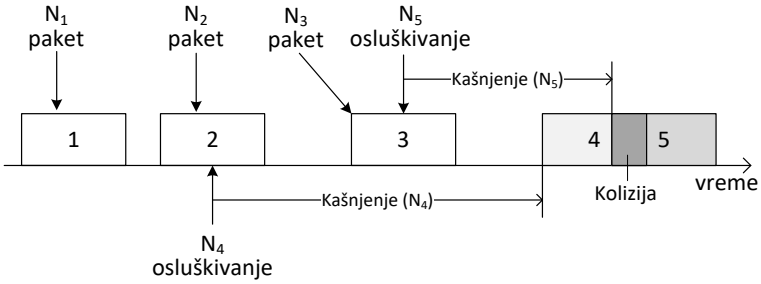
protokolu ALOH svakako nemoguće. Propusnost 0.1 znači da je u datim uslovima (tj. za dato G) samo $1/10$ raspoloživog komunikacionog kapaciteta iskorišćena za uspešne prenose paketa. U početnom delu grafikona, propusnost raste jer raste i obim ponuđenog saobraćaja, a kolizije su, zbog malog G, i dalje retka pojava. Zato je u tom delu svaki prenos paketa uspešan. S druge strane, pri većem G, uređaji često pokušavaju slanje svojih paketa, što dovodi do učestalih kolizija. Vreme se više ne troši samo na uspešne prenose već i na prenose koji se odbacuju zbog pojave kolizija. Vidimo da za ekstremno veliko G sistem troši (tačnije, baca) gotovo celokupni raspoloživi komunikacioni kapacitet na neuspešne prenose. Pri ovim uslovima, mreža je, praktično, neupotrebljiva. Takođe, na Sl. 12 vidimo da je maksimalna propusnost *Slotted* ALOHA protokola, 0.386, tj. duplo veća od maksimalne propusnosti *Pure ALOHA*. Propusnost 0.386 znači da *Slotted* ALOHA mreža, u najboljem slučaju, može da prenese, u proseku, najviše 0.386 paketa po slotu, bez obzira na iznos ponuđenog saobraćaja u mreži.



Sl. 12 Propusnost protokola *Pure* ALOHA i *Slotted* ALOHA u zavisnosti od ponuđenog saobraćaja

5.3.2 CSMA

Protokoli iz kategorije CSMA (*Carrier Sense Multiple Access*) su rezultat nastojanja da se poboljšaju performanse ALOHA protokola. Niska propusnost ALOHA je posledica učestalih kolizija pri povećanom iznosu ponuđenog saobraćaja. Dakle, jedan način za povećanje propusnosti bi svakako bio da se na neki način preduprede kolizije u deljivom bežičnom medijumu. Najjednostavniji način za sprečavanje kolizija je da mrežni uređaji, pre emitovanja paketa, prosto, osluškuju komunikacioni kanal. Ukoliko medijum nije slobodan, jer neki drugi uređaj trenutno emituje svoje podatke, uređaj se povlači na neko (slučajno odabrano) vreme, a zatim ponovo pokušava.

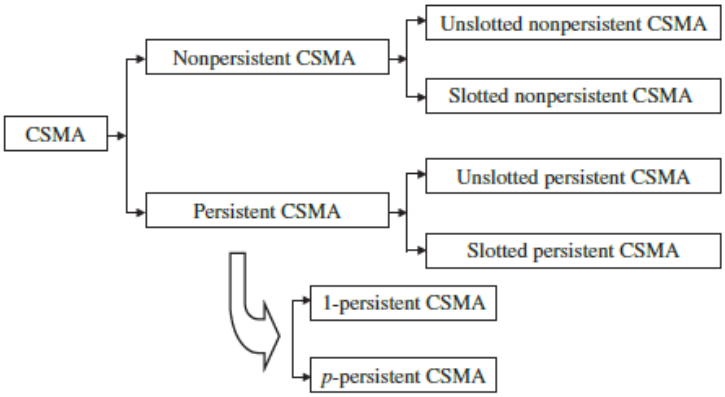


Sl. 13 CSMA

Princip rada osnovnog CSMA protokola je ilustrovan na Sl. 13. Vidimo da uređaj N_4 pokušava prenos u vreme emitovanja paketa „2“. N_4 osluškuje medijum i detektuje ovu emisiju i zato odlaže slanje na

izvesno vreme, zatim ponovo osluškuje medijum i počinje emitovanje svog paketa „4“ jer je medijum slobodan. Slično, prvi pokušaj emitovanja uređaja N_5 je neuspešan zbog prenosa paketa „3“ koji je u toku. N_5 pravi pauzi i ponovo pokušava. Međutim, uprkos tome što je N_5 osluškivao kanal pri ponovnom pokušaju, ipak dolazi do kolizije između paketa „4“ i „5“. Zbog čega? Razlog bi mogao biti taj da je rastojanje između N_4 i N_5 veliko i da N_5, prosto, nije čuo transmisiju uređaja N_4 (npr. N_4 i N_5 se nalaze na suprotnim stranama centralnog čvora u mreži zvezdaste topologije). Drugi razlog kada može doći do kolizije, uprkos tome što uređaji osluškuju medijum, je konačna brzina propagacije radio talasa. Naime, može se desiti da N_5 detektuje slobodan kanal iako je neki drugi uređaj, N_4, već započeo svoje emitovanje, ali emitovani radio talas još uvek nije stigao do N_5. Ovaj slučaj bi izazvao potpunu koliziju paketa, što svakako nije slučaj u primeru na Sl. 13.

Osluškivanje medijuma je poznato i kao osluškivanje nosioca (*carrier sense*), od čega i potiče skraćenica CSMA. (Noseći signal, tj. *carrier*, je, kao što znamo, visokofrekventni signal koji je modulisan informacijom koja se prenosi.). Postoji nekoliko varijanti osnovnog CSMA mehanizma. Na Sl. 14 je prikazana odgovarajuća klasifikacija.



Sl. 14 Klasifikacija CSMA protokola

Neperzistentni CSMA

Neperzistentni CSMA protokol radi upravo onako kako je opisana osnovna CSMA varijanta. Uređaj koji ima paket za slanje osluškuje medijum i ako je medijum zauzet odustaje od slanja i pravi pauzu slučajnog trajanja pre ponovnog osluškivanja medijuma. „Neperzistentan“ se odnosi na osobinu protokola da ne istrajava u osluškivanju čekajući da se završi tekuća transmisija, već, ako je medijum zauzet, prekida osluškivanje i pravi pauzu. Ovakva strategija omogućava uređaju da tokom ove pauze isključi svoj RF transiver i tako uštedi energiju.

Kao kod ALOHA, postoje dve podvarijante neperzistentnog CSMA: *slotted* i *unslotted*. Razlika je u tome što je kod *slotted* CSMA vreme podeljeno na vremenske slotove fiksnog trajanja i transmisija paketa može da počne samo na početku slota. Kod *unslotted* CSMA, nema slotova i uređaj može da počne transmisiju u bilo kom trenutku. U oba slučaja, slobodan medijum je, naravno, preduslov za transmisiju. Takođe, u oba slučaja, pauza nakon što je detektovan zauzet medijum je slučajnog trajanja, samo što kod *slotted* varijante trajanje pauze mora biti jednaka celobrojnom umnošku trajanja slota.

1-perzistentni CSMA

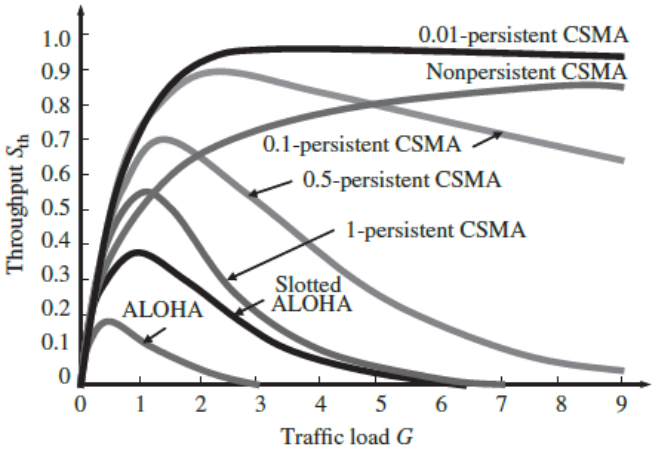
U ovoj varijanti protokola CSMA, ako je medijum zauzet, uređaj nastavlja sa osluškujem i počinje emitovanje svog paketa odmah nakon što medijum postane slobodan. „Perzistentan“ (ili istrajan) ukazuje na to da uređaj neprekidno osluškuje medijum čekajući da se tekuća transmisija završi. „1-Perzistentan“ znači da će uređaj početi transmisiju uvek, tj. sa verovatnoćom $p = 1$, kada primeti da

je medijum slobodan. Naravno, kod ovog protokola će uvek doći do kolizije ukoliko dva ili više uređaja čekaju oslobađanje medijuma, budući da će svi oni početi s transmisijom u istom trenutku kada se medijum oslobodi.

p-perzistentni CSMA

Kod ove varijante protokola CSMA, vreme je podeljeno na slotove i bilo koja transmisija može da počne samo na početku slota. Kao i prethodno, uređaj mora da osluškuje medijum pre slanja svog paketa. Ako je medijum zauzet, uređaj čeka na početak sledećeg slota i ponovo osluškuje medijum. Ako je medijum ponovo zauzet, uređaj pravi novu pauzu trajanja jednog slota i ponovo osluškuje medijum. Ako je na početku slota medijum slobodan, uređaj počinje transmisiju sa verovatnoćom p, odnosno odlaže transmisiju za sledeći slot sa verovatnoćom $1-p$. U sledećem slotu, ako je medijum slobodan, uređaj postupa na isti način – počinje transmisiju sa verovatnoćom p, ili je odlaže za sledeći slot, sa verovatnoćom $1-p$. Ako dođe do kolizije paketa, odnosno, ako uređaj ne primi potvrdu prijema od centralnog čvora, uređaj se povlači na neko slučajno odabrano vreme, a onda ponavlja istu proceduru. Dakle, ovde je suština u tome da uređaj neće uvek početi transmisiju nakon detekcije slobodnog medijuma (kao što je to slučaj kod 1-perzistentnog CSMA), već odluku o tome da li emitovati ili ne donosi „bacanjem novčića“. Na ovaj način se otklanja većina kolizija koje nastaju u slučajevima kada dva ili više uređaja čeka na oslobađanje medijum. Što je p manje, to se može očekivati da će u sistemu biti i manje kolizija. Međutim, malo p dovodi do povećanja vremena čekanja paketa, odnosno uvodi se kašnjenje u prenosu paketa zbog velike verovatnoće da će uređaj odložiti slanje paketa za sledeći slot. Takođe, ako je ponuđeni saobraćaj u mreži mali, biće čestih situacija kada samo jedan uređaj čeka na oslobađanje medijum i kada je odlaganje početka emitovanja čisto gubljenje vremena.

Na Sl. 15 je prikazan grafikon zavisnosti propusnosti od ponuđenog saobraćaja za različite MAC protokole sa nadmetanjem. Kao što vidimo, CSMA, kao kompleksniji mehanizam, obezbeđuje značajnu veću propusnost od ALOH protokola. Prema ovom grafikonu, *p*-perzistentni CSMA sa malim p, omogućava gotovo 100%-no iskorišćenje raspoloživog komunikacionog kapaciteta. Međutim, kao što je već napomenuo, treba imati na umu da malo p unosi veliko kašnjenje paketa.



Sl. 15 Propusnost različitih MAC protokola sa nadmetanjem u zavisnosti od ponuđenog saobraćaja

5.3.3 CSMA/CA

CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) je MAC mehanizam (tačnije, set mehanizama) koji delje poboljšava performanse CSMA. Odrednica „CA“ (*Collision Avoidance*) se odnosi na izbegavanje kolizija, što znači da ovaj protokol pokušava da, koliko god je to moguće, predupredi nastanak kolizija, umesto da sanira posledice kolizija. Koncipiran je po ugledu na MAC protokol CSMA/CD, koji se koristi kod žičanih LAN (*Local Area Networks*), konkretno kod Ethernet LAN,

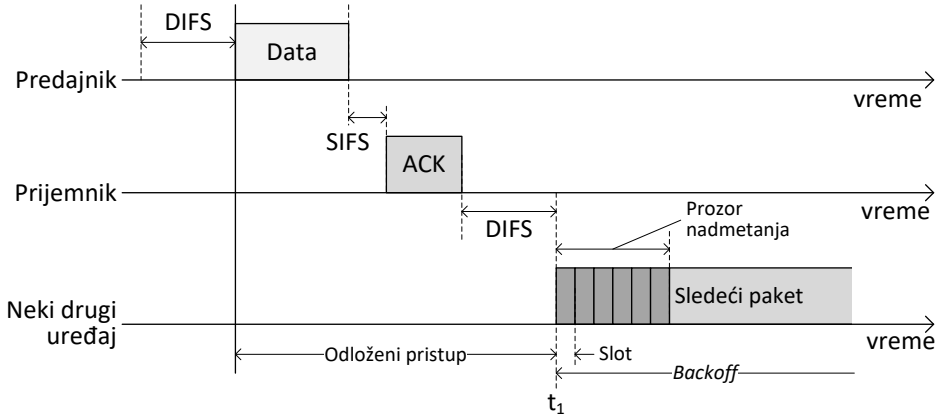
gde se „CD“ (*Collision Detection*) odnosi na detekciju kolizija. Naime, uređaji povezani u Ethernet LAN imaju mogućnost detektovanja pojave kolizije za vreme dok šalju svoje podatke. U slučaju detektovane kolizije, uređaj momentalno prekida slanje i preduzima određene dalje korake. U bežičnoj komunikaciji, „CD“ tehnički nije moguće izvesti. Čvor ne može istovremeno da emituje i prima radio signal, odnosno da za vreme emitovanja osluškuje medijum i procenjuje da li u „etru“, osim njegove postoji i neka druga transmisija. Zbog toga se u bežičnoj komunikaciji „CD“ zamenjuje sa „CA“.

Uprkos tome što ne može da detektuje koliziju, predajni uređaj ipak mora da ima informaciju o tome da li je prenos uspešno obavljen, odnosno da li je prijemnik ispravno primio poslati paket podataka. Ovo se postiže paketom potvrde (ACK) koji prijemni uređaj šalje predajnom uređaju odmah nakon uspešnog prijema kompletnog paketa podataka. Zapravo ne baš odmah, već nakon kratkog kašnjenja, tzv. SIFS (*Short Inter-Frame Space*), koje je reda desetak mikrosekundi, a uvodi se da bi uređaj koji je do tog trenutka emitovao paket imao dovoljno vremena da svoj RF primopredajnik postavi u režim prijema. Dakle, nakon završenog prenosa paketa, predajni uređaj se prebacuje na prijem i čeka na prijem ACK paketa, određeno fiksno vreme. Izostanak ACK paketa može biti posledica kolizije koja je nastupila prilikom prenosa paketa podataka ili prilikom prenosa samog ACK paketa. Protokol ne pravi razliku između ove dve situacije i izostanak ACK paketa smatra indikacijom neuspešnog prenosa, koji treba ponoviti.

Kod CSMA/CA, osnovni mehanizam za sprečavanje kolizija je osluškivanje medijum, kao i u bazičnim verzijama CSMA protokola. Kod CSMA/CA osluškivanje je perzistentno, što znači da uređaj koji ima paket za slanje neprekidno nagleda medijum čekajući da se oslobodi. Međutim, najveći broj kolizija nastaje upravo nakon što se završi tekuća transmisija, u situacijama kada više uređaja čeka slobodan medijum da bi započeli svoje emitovanje. Prethodno smo videli kako se *p*-perzistentnim CSMA rešava, tačnije, ublažava, ovaj problem. CSMA/CA ide korak dalje i uvodi nešto složeniji mehanizam sprečavanja kolizija. Prvo, uslov za slobodan medijum je da čvor nije detektovao transmisiju u vremenu DIFS (*Distributed Interframe Space*). Ovo vreme se definiše konkretnim protokolom, ali tako da važi $DIFS > SIFS$. Na taj način se obezbeđuje da čvor koji čeka na slobodan medijum neće početi svoju transmisiju pre nego što je prenet ACK paket za upravo završen prenos. Ovo je ilustrovano na Sl. 16. Dok uređaj označen kao „Predajnik“ emituje svoj paket “Data“, svi ostali uređaji u mreži, koji imaju pakete za slanje, perzistentno čekaju da se ova transmisija završi. Nakon prenetog paketa “Data“, sledi pauza trajanja SIFS, a zatim i transmisija ACK paketa od strane odredišnog uređaja “Prijemnik“. Uređaji koji čekaju (označeni na Sl. 16 kao „Neki drugi uređaji“), detektovali su prestanak transmisije paketa “Data“, ali s obzirom da imaju obavezu da dodatno čekaju vreme DIFS, ni jedan od njih neće početi emitovanje. Medijum se smatra slobodnim tek kada se završi prenos ACK paketa i protekne dodatno vreme DIFS u kome nema nikakvih transmisija. Recimo da se ovo desilo u trenutku t_1. U ovom trenutku počinje vremenski period koji se naziva prozor nadmetanja (CW - *contention window*).

Uređaj sa paketom koji čeka na slanje, neće započeti prenos u trenutku t_1, jer bi to izvesno dovelo do kolizije sa drugim čvorovim koji su takođe čekali na oslobađanje medijuma. Umesto momentalne transmisije, uređaj nasumično bira trajanje perioda dodatnog čekanja (*backoff*) u okviru prozora nadmetanja. CW se sastoji iz određenog broja kratkotrajnih vremenskih slotova fiksnog trajanja. Uređaj zapravo nasumično bira redni broj slota u kome će započeti emitovanje i tim brojem inicijalizuje svoj *backoff* brojač (*backoff counter*). Sa svakim proteklim slotom, *backoff* brojač odbrojava za 1 unazad. Dok čeka da stanje *backoff* brojača postane 0, uređaj neprekidno osluškuje medijum. Ukoliko detektuje transmisiju u medijumu, uređaj zaustavlja svoj *backoff* brojača i odustaje od transmisije, tj. ponovo čeka na oslobađanje medijum (ponavlja prethodno opisanu proceduru). Praktično, tokom prozora nadmetanja, uređaji se nadmeću za pravo pristupa medijumu, a u tom nadmetanju pobeđuje onaj uređaj koji je u prozor nadmetanja ušao sa najmanjom vrednošću *backoff* brojača. Samo

pobednik stiče pravo emitovanja, dok svi ostali čekaju na početak sledećeg prozora nadmetanja da bi ponovo pustili u rad svoje *backoff* brojače. Naravno, i u ovoj šemi postoji mogućnost kolizije – onda kad bar dva uređaja uđu u nadmetanje sa istom, najmanjom, vrednošću *backoff* brojača.

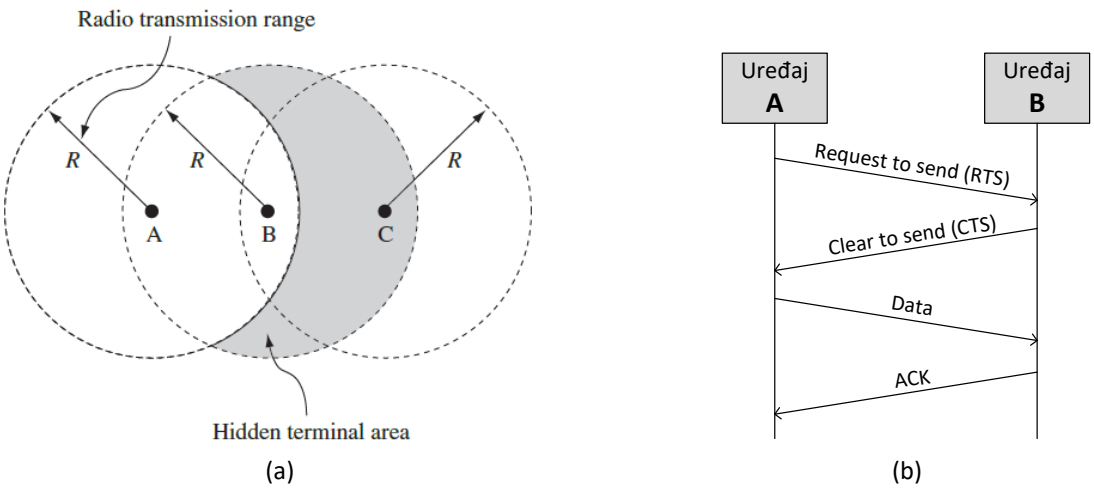


Sl. 16 CSMA/CA

Svaki čvor ima svoj CW, čije trajanje nije fiksno (u smislu broja slotova) već se dinamički menja. Podrazumevano, dužina CW je mala – tek nekoliko slotova. Međutim, nakon kolizije (izostanak ACK paketa), uređaj duplira dužinu svog CW, i nastavlja dupliranje sa svakom uzastopnom kolizijom. Dupliranje traje sve dok se ne dostigne maksimalno dopuštena dužina CW-a, koja se nakon toga više ne menja. Tek kada dobije ACK potvrdu za poslati paket, čvor vraća dužinu CW-a na podrazumevanu vrednost. Ovakav način rada se naziva *eksponencijalni backoff*. Opravdanje za eksponencijalni backoff je to što pojava uzastopnih kolizija ukazuje da trenutno u mreži veći broj čvorova pokušava slanje, što zahteva duži prozor nadmetanja – smanjuje se verovatnoća da će dva čvora izabrati isti slot. S druge strane, nije dobro da CW stalno bude dugačko, jer se tako prolongira početak emitovanja i usporava komunikacija, pa se zato CW vraća na početnu vrednost nakon uspešno prenetog paketa.

CSMA/CA sa RTS/CTS

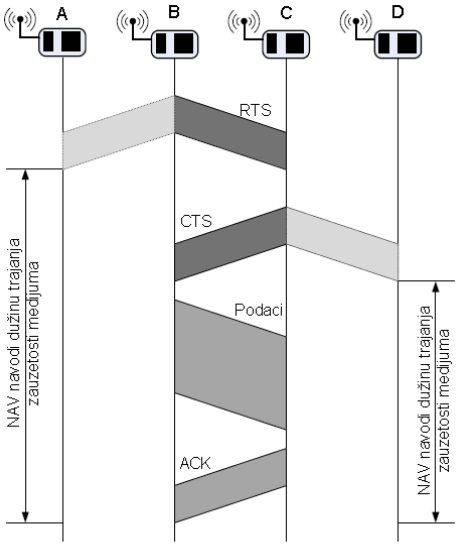
Problem skrivenih terminala. Mehanizam nadmetanja iz protokola CSMA/CA značajno smanjuje mogućnost kolizija, ali ipak ne rešava jedan fundamentalni problem koji je karakterističan za bežične mreže, a koji je poznat pod nazivom problem skrivenih terminala (*hidden terminal problem*). Skriveni terminali su uređaji koji pripadaju istoj bežičnoj mreži, imaju zajedničkog suseda, ili susede, ali se međusobno nalaze izvan dometa svojih radio signala. Problem skrivanih terminala nastaje kada dva ili više skrivenih terminala istovremeno emituju. Na primer, na Sl. 17(a), uređaji (čvorovi) A i C oba mogu da komuniciraju sa čvorom B, ali ne i među sobom, jer su na previše velikom međusobnom rastojanju. Odnosno, čvor C ne može da čuje emitovanje čvora A, kao što ni A ne čuje emitovanje čvora C. Zato je C skriven terminal za A, kao što je i A skriven terminal za C. Na Sl. 17(a), R označava domet radio transmisije. Osnovni CSMA/CA ne može da reši problem skrivenih terminala kada čvorovi A i C istovremeno šalju svoje pakete čvoru B. Recimo da je C prvi počeo sa transmisijom i da je u toku ove transmisije čvor A takođe poželeo da pošalje paket čvoru B. Čvor A osluškuje medijum i pošto ne detektuje nikakvu transmisiju, počinje sa predajom svog paketa, što naravno izaziva koliziju u tački čvora B. Dakle, CSMA/CA je u ovim okolnostima praktično neupotrebljiv.



Sl. 17 (a) Problem skrivenih terminala i (b) osnovna RTS/CTS procedura

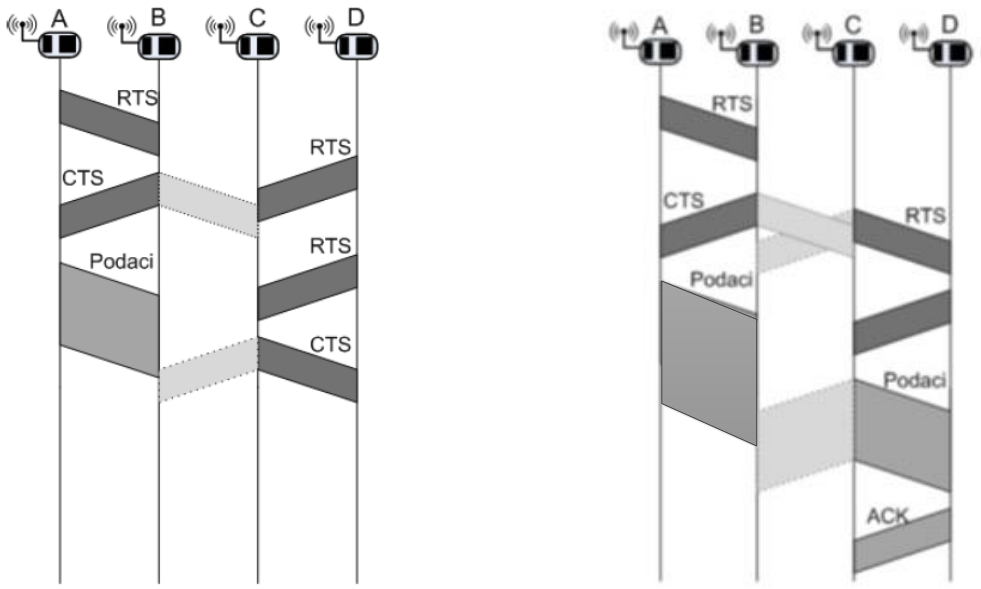
RTD/CTS procedura. Problem skrivenih terminala se može rešiti proširenjem CSMA/CA protokola tzv. RTS/CTS (*request to send/clear to send*) procedurom. RTS/CTS je u suštini procedura usaglašavanja (*handshake*) između predajnog i prijemnog čvora pre samog početka prenosa paketa podataka. Recimo da uređaj A želi da pošalje paket podataka čvoru B (Sl. 17(b)). Procedura počinje tako što uređaj A šalje uređaju B kratak paket RTS (zahtev za slanje) kojim ga obaveštava o svojoj nameri da mu pošalje paket podataka. Na primljeni RTS paket, uređaj B, ako je voljan da primi paket podataka, odgovara, takođe kratkim paketom CTS. Uređaj A, po prijemu paketa CTS, šalje paket podataka uređaju B, a ovaj mu odgovara paketom ACK. Ovde je poenta u tome da će CTS paket primiti ne samo uređaj A kome je taj paket namenjen, veći i svi ostali uređaji koji su u radio dometu uređaja B, pa i skriveni terminali uređaja A. Dakle, kada uređaj C, koji je skriveni terminal uređaja A, primi B-ov CTS, on će zna da sledi transmisija ka uređaju B, koju neće čuti, ali će znati da postoji i zbog toga će se uzdržati od emitovanja.

Sada se postavlja se pitanje, kako čvor C zna do kada će trajati transmisija koju ne čuje? Jedna mogućnost je da C čeka na ACK koji će čvor B poslati čvoru A nakon prijema paketa podataka. Međutim, šta ako C ne primi ACK (zbog kolizije ili, prosto, greške u prenosu)? Uz to, pošto ne zna trajanje transmisije, C mora sve vreme aktivno da nadgleda medijum u očekivanju ACK paketa i da tako troši energiju. Rešenje ovog problema se sastoji u tome da kontrolni paketi, RTS i CTS, između ostalog nose i informaciju o trajanju predstojeće transmisije paketa podataka. To omogućava uređaju C (na Sl. 18) da nakon prijema RTS paketa dobije i informaciju o trajanju celokupne transmisije (paket podataka plus AKC). Sa ovom informacijom na raspolaganju, C može da isključi svoj RF primopredajnik i ponovo ga uključi kad transmisija prođe. Slično postupa i D, koji je informaciju o vremenu transmisije dobio preko CTS paketa.



Sl. 18 RTS/CTS sa NAV

Ovaj način rada se naziva virtuelno osluškivanje (NAV - *Network Allocation Vector*). Na Sl. 18 je ilustrovan rad CSMA/CA as RTS/CTS i NAV. Kod protokola zasnovanih na CSMA, uobičajeno je da i svaki paket podataka (ne samo RTS i CTS) nosi u svom zaglavlju informacija o trajanju transmisije. Ovo omogućava korišćenje NAV tehnike i onda kada RTS/CTS mehanizam nije u upotrebi.



(a) (b)

Sl. 19 Dva problema sa RTS/CTS procedurom

Procedura RTS/CTS nije idealna, u smislu da ne predstavlja apsolutnu zaštitu od pojave kolizija uzrokovanih problemom skrivenih terminala. Postoje određeni, doduše maloverovatni scenariji, u kojima, uprkos primeni RTS/CTS, ipak dolazi do kolizija. Dva takva scenarija su prikazana na Sl. 19. U prvom scenariju (Sl. 19(a)), pratimo dve „RTS-CTS-Podaci-ACK“ transakcije, gde je jedna između uređaja A i B i druga između C i D. Uređaj A je inicijator prve, a uređaj D druge transakcije. Čvor C ne čuje RTS koje A šalje čvoru B, ali zato čuje CTS koje uređaj B šalje uređaju A, što bi trebalo da odvrati uređaj C od učešća u komunikaciji sa D. Međutim, desilo se to da je D poslao RST paket uređaju C baš u vreme transmisije CTS paketa od B ka A. Zbog toga se CTS paket uređaja B i RTS paket uređaja D sudaraju u tački uređaja C i C ne prima ni jedan od ova dva paketa. Uređaj D koji nije dobio CTS potvrdu od C, ponovo će, posle izvesnog vremena, poslati RTS. Sada nema kolizije u tački uređaja C i C prima RTS. S obzirom da nije svestan transmisije između A i B, uređaj C odgovara slanjem CTS paketa, što izaziva koliziju sa paketom podataka u tački uređaja B.

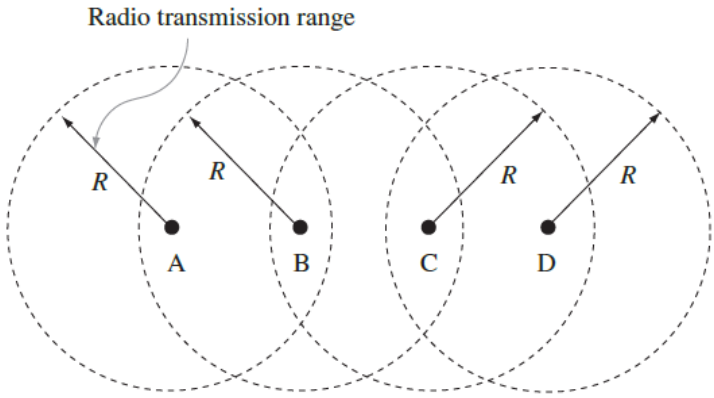
Kolizija u scenariju na Sl. 19(b) je posledica polu-dupleks rada RF primopredajnika: RF primopredajnik može biti u režimu predaje ili prijema, ali ne i u oba režima u isto vreme. To znači da dok uređaj C šalje RTS paket uređaju D, on neće biti u mogućnosti da primi CTS paket koji, u to isto vreme, uređaj B šalje uređaju A (kao ni što uređaj B neće primiti RTS paket koji uređaj C šalje uređaju D). Zbog toga, B i C nastavljaju svoje transakcije što, kao što se vidi na slici, dovodi do kolizije paketa u tački uređaja B.

RTS/CTS procedura ima i drugih nedostataka. Prvo, troši vreme, pa time i raspoloživ komunikacioni kapacitet. Ovo je posebno izraženo u situacijama kada se prenose kratki paketi podataka, što je tipično slučaj u mrežama jednostavnih uređaja (senzori i sl.). Drugo, dovodi do pojave tzv. izloženih terminala.

Problem izloženih terminala

Protokol CSMA/CA sa RTS/CTS procedurom, koji u velikoj meri otklanja problem skrivenih terminala, izaziva jedan novi problem, koji je poznat pod nazivom problem izloženih terminala (*exposed terminal problem*). Primer je dat na Sl. 20. U ovom mrežnom scenariju, uređaji A i B mogu međusobno da komuniciraju. Isto važi za uređaje B i C i uređaje C i D. Međutim, A ne čuje C i D, kao što D ne čuje A i B. Pretpostavimo da uređaj B namerava da pošalje paket podataka uređaju A i da mu zbog toga prvo šalje RTS paket. Ovaj paket ne prima samo A, kome je namenjen, već i svi čvorovi u dometu uređaja

B, pa i uređaj C. Zbog toga će se C uzdržati od slanja podataka uređaju D, iako prenos između C i D ne bi smetao prijemu podataka kod uređaja A. Upravo ovo nepotrebno uzdržavanje od emitovanja predstavlja problem izloženih terminala. Posledica ovog problema je to što obično dovodi do smanjenog protoka podataka u mreži.



Sl. 20 Problem izloženih terminala

5.4 Vodič za učenje

- Problem višestrukog pristupa. Osnovna klasifikacija MAC protokola

Mac protokoli sa statičkom alokacijom resursa

- Opšti princip. Koji resursi su podložni raspodeli
- TDMA. Princip. Prednosti. Nedostaci, sinhronizacija, latencija, efikasnost
- FDMA. Princip. FDMA u radio-difuznim, celularnim mrežama, WPAN i WLAN mrežama. Prednosti i nedostaci
- CDMA. Opšti princip (Sl. 6 i objašnjenje).
    - Direktna sekvenca. Princip (Sl. 7). Kodne sekvence i ortogonalnost kodnih sekvenci. (Vošove sekvenci i način konstrukcije – nije neophodno)
    - Frekventno skakanje. Princip. Brzo i sporo frekventno skakanje

MAC protokoli sa nadmetanjem

- Razlika između implicitnih i eksplicitnih strategija za nadmetan

ALOHA

- Postavka i princip čiste ALOHA (Sl. 10). Interval ranjivosti
- *Slotted* ALOHA. Princip (Sl. 11). Interval ranjivosti. Performanse ALOHA i *Slotted* ALOHA (nije neophodno da pamtite grafikon (Sl. 12), ali bi trebalo da možete da objasnite zavisnost propusnosti od ponuđenog saobraćaja i zašto je *Slotted* ALOHA bolji od čiste ALOHA).

CSMA

- Princip osnovnog CSMA (SL. 13)
- Razlika između perzistentnog i neperzistentnog CSMA
- Neperzistentni CSMA
- 1-perzistentni i p-perzistentni CSMA. Uticaj parametra p na propusnost i latenciju

CSMA/CA

- Potrebno je da znate sledeće aspekte ovog protokola (SL. 16):
    - Potvrđivanje (ACK) i SIFS
    - Perzistentno osluškivanje i uslov za slobodan mediju (DIFS)
    - Prozor nadmetanja (CW - *contention window*) i backoff procedura.
    - Ponovljene kolizije i manipulacija dužinom prozora nadmetanja (eksponencijalni *backoff*)

RTS/CTS

- Problem skrivenih terminala i opšta RST/CTS procedura (Sl. 17)
- Kako RTS/CTS procedura otklanja problem skrivenih terminala
- RTS/CTS sa NAV
- Dva scenarija kada RTS/CTS ne može da spreči koliziju, objašnjenje Sl 19
- Problem izloženih terminala

- ♦ ♦ ♦ -