



Libraries and Learning Services

University of Auckland Research Repository, ResearchSpace

Version

This is the publisher's version. This version is defined in the NISO recommended practice RP-8-2008 <http://www.niso.org/publications/rp/>

Suggested Reference

Berber, S. M. (2014). Theoretical analysis and simulation of a code division multiple access system (CDMA) for secure signal transmission in wideband channels. *Military Technical Courier / Vojnotehnicki glasnik*, 62(3), 37-58. doi: [10.5937/vojtehg62-5487](https://doi.org/10.5937/vojtehg62-5487)

Copyright

Items in ResearchSpace are protected by copyright, with all rights reserved, unless otherwise indicated. Previously published items are made available in accordance with the copyright policy of the publisher.

This is an open-access article distributed under the terms of the [Creative Commons Attribution License](https://creativecommons.org/licenses/by/4.0/)

For more information, see [General copyright](#), [Publisher copyright](#), [SHERPA/RoMEO](#).

TEORIJSKA ANALIZA I SIMULACIJA SISTEMA SA KODNOM RASPODELOM KANALA (CDMA) ZA ZAŠTIĆENI PRENOS SIGNALA U ŠIROKOPOJASNIM KANALIMA

Stevan M. Berber

The University of Auckland, ECE Department, New Zealand

DOI: 10.5937/vojtehg62-5487

OBLAST: telekomunikacije, bežični komunikacioni sistemi
VRSTA ČLANKA: originalni naučni članak

Sažetak:

Haotične kodne sekvence mogu da povećaju otpornost na presretanje i obezbede tajnost u prenosu signala. Sistemi sa kodnom raspodelom kanala (CDMA), bazirani na primeni haotičnih sekvenci, u slučaju prisutnosti ravnog fedinga i šuma u kanalu prenosa, jako su dobro ispitani. Međutim, ovi sistemi u slučaju rada u širokopoljaskim kanalima, koji u sebi imaju frekvencijski selektivni feding i beli Gausov šum, nisu ispitani na nivou na kojem bi se razumela njihova praktična primenljivost. Ovaj članak prezentira detaljan matematički model CDMA sistema koji je baziran na haotičnim kodnim sekvencama. Pri teorijskoj analizi sistema svi signali su predstavljeni u diskretnom vremenu. Koristeći teoriju stohastičkih procesa diskretnog vremena izvedeni su izrazi za verovatnoću greške bita u zatvorenom obliku. Radi upoređenja uskopojasnih i širokopoljaskih sistema posebno su izvedeni ovi izrazi za oba ova sistema. Ispitana je mogućnost primene tehnike interlivinga, što je pokazalo da ova tehnika može znatno da poboljša verovatnoću greške bita u sistemu. Sistem je simuliran i dobijeni nalazi simulacije potvrdili su teorijski očekivane rezultate. Moguća poboljšanja verovatnoće greške bita u širokopoljaskom kanalu, u prisustvu i odsustvu interlivinga, kvantitativno su izražena u zavisnosti od slučajnog kašnjenja i broja učesnika u sistemu. Za analizu sistema korišćen je pojednostavljeni model širokopoljaskog kanala koji je preporučan za moderne bežične mreže.

Ključne reči: sistemi bazirani na haosu; siguran prenos signala; CDMA sistemi; širokopoljaski kanali; primena „interlivinga“.

Uvod

Poslednjih godina došlo je do velikog povećanja zahteva za bežičnim komunikacijama zahvaljujući napretku u razvoju mobilnih komunikacionih sistema i mreža i potrebama korisnika ovih sistema. Sledeći ove zahte-

ve, na moderne komunikacione sisteme postavljaju se strogi uslovi da istovremeno opslužuju veliki broj učesnika i da uz to obrađuju i prenose širokopojsne signale kroz složene frekvencijski selektivne komunikacione kanale.

Jedna od tehnika prenosa višeučesničkih signala zasnovana je na kodnoj raspodeli kanala, poznata pod engleskim nazivom „Code Division Multiple Access (CDMA)“, koja omogućava komunikaciju više učesnika u istom sistemu. To je ostvareno tako što je svakom učesniku dodeljena jedinstvena kodna sekvenca (engl. code or spreading sequence), koja se koristi na prijemniku datog učesnika da se izdvoji njemu namenjena informacija. Ovakvi sistemi pripadaju grupi komunikacionih sistema za prenos u proširenom spektru baziranih na primeni direktne sekvence. Za ove kodne sekvence tradicionalno se koriste binarne ortogonalne sekvence.

U ovom članku biće razvijen matematički model i simulacija CDMA sistema koji je zasnovan na primeni nebinarnih, precizno govoreći – haotičnih kodnih sekvenci. Ove sekvence po prirodi svog generisanja pripadaju slučajnim sekvencama sa beskonačnom periodičnošću, te su stoga pogodne za primenu u sistemima gde se želi povećati zaštita u prenosu učesničkih informacija. Posebno su pogodne za primenu u sistemima koji podrazumevaju povećanu tajnost i zaštitu od presretanja u prenosu informacija.

Moderni komunikacioni sistemi zahtevaju prenos signala velikim bit-skim brzinama, odnosno širokopojsnih signala. Ovaj trend u razvoju komunikacionih sistema i mreža će se nastaviti i biti jedan od glavnih pokretača istraživanja u budućnosti. Sledstveno tome, postavlja se zahtev za kanal prenosa koji treba da bude širokopojsan. Ovaj zahtev je posebno izražen u sistemima bežičnih veza u zatvorenom prostoru, gde je kanal prenosa kompleksan i karakterisan frekvencijskom selektivnošću (Saleh, Valencuela, 1987), (Balakrishnan, i dr, 2006). Primeri ovakvih sistema predstavljaju bežične senzorske mreže i višeučesnički sistemi primenjeni u zatvorenim prostorima kao što su zgrade, industrijska postrojenja ili rudnici, gde je kanal prenosa širokopojsan zbog prirode složenog prostiranja signala, kao što je potvrđeno istraživanjima u poslednjim godinama (Brennan, 1959), (Ochsner, 1978), (Kyro i dr, 2012), (Qilian, 2011).

Sistemi sa proširenim spektrom i sistemi sa kodnom raspodelom kanala, zasnovani na primeni haotičnih sekvenci, bili su predmet posebnog interesa u poslednje dve dekade. Ova istraživanja rezultirala su značajnim doprinosima u dizajnu ovih sistema (Heidari-Bateni, 1994), (Mazzini i dr, 1997), (Rovatti i dr, 1998), (Lau, Tse, 2004), (Tam i dr, 2004, pp.1868-1878), (Jovic i dr, 2006), (Kaddoum i dr, 2010), (Kaddoum i dr, 2009). Posebni problem u realizaciji ovih sistema je ostvarenje sinhronizacije kodnih sekvenci, što je pokrenulo intenzivne istraživačke aktivnosti sa naučnim doprinosima prezentiranim u brojnim publikacijama (Kolumban i dr, 1997), (Kolumban i dr, 1998), (Kolumban i dr, 2000), (Parlitz i dr, 1992), (Setti i dr, 1999), (Berber, Jovic, 2006), (Berber, 2006), (Jović i dr, 2007), (Kaddoum i dr, 2009), (Vali i dr, 2010, pp.1924-1939), (Yu-Nan, Lin, 2003), (Yu-Nan, Lin, 2005).

Sva ova istraživanja bila su osnovana na pretpostavci da je kanal prenosa informacija karakterizovan belim Gausovim šumom i ravnim fedingom. Problem razvoja sistema u proširenom spektru sa direktnom sekvencom za širokopojasni prenos signala bio je predmet analize u Oknerovom radu (Ochsner, 1978). On je razvio sistem za prenos širokopojasnog signala u osnovnom opsegu učestanosti kroz komunikacioni kanal koji je predstavljen sa M kašnjenja, gde svako kašnjenje odgovara trajanju jednog čipa u kodnoj sekvenci. Pokazano je da je moguće ostvariti smanjenje verovatnoće greške bita odgovarajućim korišćenjem potencijalno postojećeg diverzitija u ovakvom kanalu prenosa. Detaljna analiza sistema sa haotičnim sekvencama u širokopojasnim kanalima i konstrukcija prijemnika koji kombinuje zakasnele verzije signala (Rake prijemnici) prezentirana je u brojnim radovima (Rovatti i dr, 2001), (Kaddoum i dr, 2009), (Kaddoum i dr, 2012), (Rovatti i dr, 2001). Širokopojasni CDMA sistem sa direktnom sekvencom je analiziran u radu (Chen, Chen, 2001), pri čemu su koeficijenti kašnjenja kanala estimirani korišćenjem Kalmanovog filtera što je omogućilo da se izvede izraz za verovatnoću greške u opštem obliku. Sistem sa haotičnim sekvencama je prezentiran u (Cimatti i dr, 2007), gde je usvojena pretpostavka o prisutnosti termalnog šuma u kanalu prenosa i izvršeno upoređenje sistema sa klasičnim i haotičnim sekvencama.

Sistem CDMA sa direktnom sekvencom i kanalom prenosa sa kašnjenjima i fedingom definisanim Relijevim koeficijentima, bio je predmet detaljne analize u poslednje vreme (Xiao, Strom, 2010). Ovaj rad pretpostavlja poznavanje karakteristika kanala koje su dobijene pomoću estimatora kanala. Slična analiza ovog sistema prezentirana je u radu (Torrieri i dr, 2010) za slučaj kada širokopojasni kanal sadrži tri razdvojive komponente primljenog signala koje se mogu kombinovati u prijemniku radi ostvarenja diverziti prijemnika signala. U literaturi se često koriste Proakisovi modeli kanala. Jedna varijanta ovog kanala, Proakis C kanal, korišćen je u analizi CDMA sistema (Yue i dr, 2010). Sistem sa haotičnim sekvencama i prenosom u osnovnom opsegu učestanosti je analiziran nedavno (Kaddoum, Gagnon, 2012) u slučaju kanala sa belim Gausovim šumom, a zatim je analiza proširena na sistem prenosa sa modulisanim nosiocima. U (Kaddoum i dr, 2013) izvršena je analiza sistema sa više nosilaca u širokopojasnom kanalu koji je predstavljen koeficijentima fedinga i višestrukim kašnjenjima signala.

Većina referenciranih CDMA sistema baziranih na haotičnim sekvencama analizirana je u slučaju prenosa signala u osnovnom opsegu učestanosti kroz feding kanal sa belim Gausovim šumom. Sistemi sa prenosom signala u širokopojasnom kanalu praktično nisu analizirani u smislu izvođenja ključnih izraza za verovatnoću greške bita kao mere kvaliteta prenosa informacija u sistemu. Imajući na umu ove nedostatke, u ovom članku prezentirane su sledeće analize CDMA širokopojasnih sistema sa odgovarajućim doprinosima.

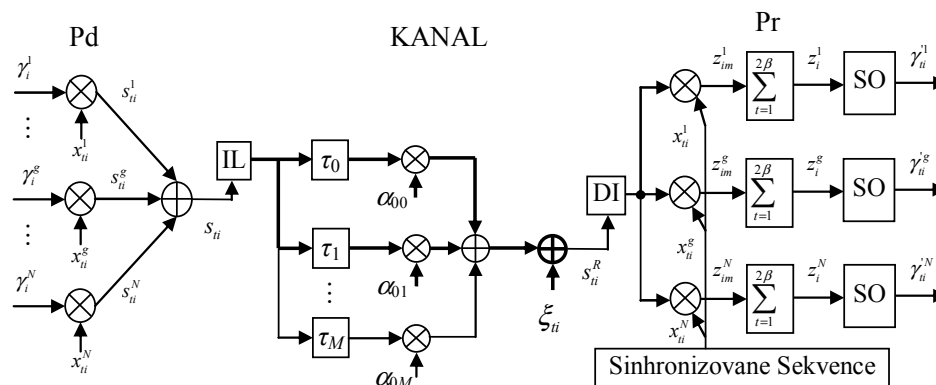
Pre svega, CDMA sistem analiziran je pod pretpostavkom da se multi-učesnički signal prenosi kroz širokopojasni kanal u kojem je prisutan Gaussov šum i frekvencijski selektivni feding. Statističke karakteristike haotičnih sekvenci prezentirane su radi osnovnog razumevanje njihove primerljivosti u CDMA sistemu. Osnovne karakteristike uskopojasnog kanala u bežičnim komunikacijama prezentirane su u vezi sa karakteristikama širokopojasnog kanala. Posebni doprinos predstavlja izvod teorijskih izraza za verovatnoću greške bita u sistemu koji su potvrđeni simulacijama sistema.

Jedna od metoda eliminacije fedinga u sistemu jeste primena blokova za interliving čipova u kodnim sekvencama (engl. chip interleaving). Za ovaj slučaj izvedeni su teorijski izrazi za verovatnoću greške koji su nedvosmisleno pokazali da ova metoda znatno smanjuje greške u kanalu sa fedingom.

Osnovna struktura komunikacionog sistema i princip rada

Blok-šema CDMA sistema sa haotičnim kodnim sekvencama za proširenje spektra signala prikazana je na slici 1. Binarni signal g -tog učesnika označen je sa γ_i^g , i predstavljen nizom binarnih vrednosti iz skupa $(+1, -1)$, gde $+1$ predstavlja binarnu jedinicu, a -1 predstavlja binarnu nulu. Svakom učesniku dodeljena je jedinstvena haotična čip- sekvenca označena sa x_{ti}^g . Broj čipova koji se koristi za proširenje spektra jednog bita za učesnike poruke predstavlja procesno pojačanje sistema, koje je označeno sa 2β .

U ovom radu korišćene su kodne sekvence generisane posredstvom Čebiševljevih mapa. Dobijene sekvence normalizovane su tako da imaju srednju snagu jednaku jedinici radi mogućeg upoređenja haotičnih i binarnih sistema.



Slika 1 – Blok-šema CDMA sistema sa haotičnim kodnim sekvencama
Figure 1 – Block-schematic of a CDMA system with chaotic code sequences

Preciznije govoreći, korišćena je logistička mapa koja definiše čipove sekvence sledećom rekurzivnom formulom:

$$x_{ti}(n+1) = 1 - 2x_{ti}(n).$$

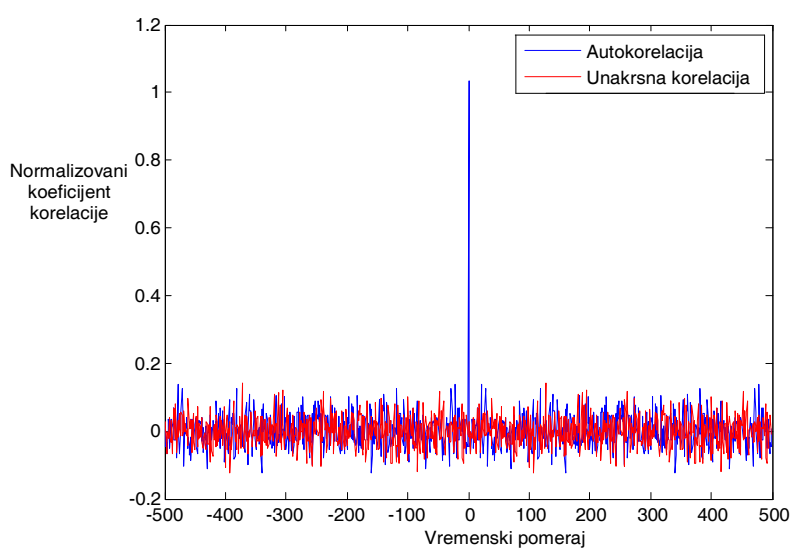
Funkcija gustine ove mape, sa normalizovanim vrednostima generisanih vrednosti čipova da se obezbedi jedinična snaga signala, definisana je izrazom (Berber, Feng, 2013)

$$f_{x_{ti}}(x_{ti}) = \frac{1}{\pi\sqrt{2-x_{ti}^2}}, \text{ for } -\sqrt{2} \leq x_{ti} \leq \sqrt{2},$$

koja se može predstaviti grafom simetričnim u odnosu na koordinatni početak i ima sledeće momente: $E\{x_{ti}\}=0$, $E\{x_{ti}^2\}=1$ and $E\{x_{ti}^4\}=3/2$ (Berber, Feng, 2013). Za različite početne vrednosti dobijaju se različite sekvence koje su međusobno ortogonalne. Dakle, sekvence čipova koje mapa generiše imaju izražen maksimum u korelacionoj funkciji i male vrednosti u funkciji unakrsne korelacije. Na slici 2 prikazane su ove dve funkcije koje potvrđuju navedene korelacione osobine.

Množenjem učesničkih bita γ_i^g sa kodnim sekvencama x_{ti}^g za svaki g dobijaju se učesnički signali s_{ti}^g prema sledećem izrazu:

$$s_{ti}^g = \gamma_i^g x_{ti}^g = \begin{cases} -1 \cdot x_{ti}^g & \gamma_i^g = -1 \\ +1 \cdot x_{ti}^g & \gamma_i^g = +1 \end{cases}$$



Slika 2 – Korelaciona funkcija i funkcija unakrsne korelacije haotične sekvence definisane početnim uslovom logističke mape

Figure 2 – Correlation and crosscorrelation functions for a chaotic sequence that is defined by the initial condition of a logistic map

gde je kodna sekvenca jednog bita g -tog korisnika izražena u ovom vidu $x_i^g = (x_1^g, x_2^g, \dots, x_{2\beta^g})$. Signali svih N učesnika sabrani su na nivou čipova, produkujući predajni signal

$$S_{ii} = \sum_{g=1}^N S_{ii}^g = \sum_{g=1}^N \gamma_i^g x_{ii}^g, \quad (1)$$

koji se prenosi kroz komunikacioni kanal sistema, kao što se vidi na slici 1. Ovde t označava poziciju čipa u i -tom bitu poslanih poruka svih učesnika.

Komunikacioni kanal definisan je koeficijentima fedinga, kašnjenjima i belim Gausovom šumom. Impulsni odziv ovog kanala, u najopštijem obliku, predstavljen je izrazom:

$$h(n) = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \alpha_{kj} e^{j\phi_{kj}} \delta(n - \tau_j - T_{kj}) \quad (2)$$

gde je α_{kj} koeficijent Rejljevog fedinga, ϕ_{kj} je fazni pomeraj, τ_{kj} je kašnjenje klastera i T_{kj} je kašnjenje signala unutar klastera. Indeks j određuje broj klastera prema notaciji za širokopojasne kanale (Saleh, Valencuela, 1987), (Balakrishnan, i dr., 2006), odnosno broj primarnih i sekundarnih kanala prema notaciji u ovom radu, dok k označava broj primljenih signala u svakom klasteru prema notaciji za širokopojasne kanale (Saleh, Valencuela, 1987), (Balakrishnan, i dr., 2006), odnosno broj potkanala prema notaciji u ovom radu. U sledećoj analizi kanal će se pojednostaviti i predstaviti jednim primarnim i jednim sekundarnim kanalom bez potkanala, kao što je prikazano na slici 1.

Koeficijenti fedinga imaju Relijevu rapodelu definisanu funkcijom gustine:

$$f_{\alpha}(\alpha) = \frac{\alpha}{b^2} e^{-\alpha^2/2b^2}$$

sa srednjom vrednošću $\eta_{\alpha} = b(\pi/2)^{1/2}$, $\eta_{\alpha^2} = 2b^2$ varijansom (disperzijom) $\sigma_{\alpha^2} = b^2(4-\pi)/2$. Kašnjenje u kanalu ima eksponencijalnu distribuciju:

$$f_{\tau}(\tau) = \lambda e^{-\lambda\tau}$$

sa srednjom vrednošću $1/\lambda$ i srednjom kvadratnom vrednošću $1/\lambda^2$. Ove distribucije definisane su u radovima (Saleh i Valencuela, 1987), (Balakrishnan, i dr., 2006).

U prijemniku se primljeni multiučesnički signal koreliše sa lokalno generisanom i sinhronizovanom haotičnom sekvencom koja odgovara željenom korisniku. Rezultat ove korelacije je slučajna vrednost z_i^g , koja teorijski predstavlja jednu realizaciju diskretne slučajne varijable Z_i^g , na osnovu čije vrednosti se donosi odluka o poslanom binarnom simbolu. Ako je ova varijabla odluke $z_i^g > 0$ (pozitivna korelacija) onda je estimirani primljeni bit +1, dok je za $z_i^g \leq 0$ (negativna korelacija) estimirani primljeni bit -1. Iako su signali svih učesnika sadržani u prijemnom signalu, korelacija sa lokalnom učesničkom kodnom sekvencom daće dovoljno veliku vrednost koja će voditi korektnoj odluci zbog osobine ortogonalnosti haotičnih sekvenci. Međutim, postojaće, takođe, deo varijable odluke Z_i^g koji je rezultat unakrsne korelacije lokalno generisane učesničke sekvence i sekvenci koje koriste ostali učesnici u sistemu. Ovaj deo varijable odluke zove se međuučesnička interferencija, koja će biti posebno ispitana u toku prezentacije rada prijemnika sistema.

Sistem sa ravnim fedingom u uskopojasnom kanalu

Radi kompletnosti prezentacije problema prenosa signala u CDMA sistemima, analiza sistema počće prezentacijom prenosa u kanalu sa ravnim fedingom. Kanal je uskopojasan u slučaju kada frekvencijski opseg signala ne prelazi koherentni opseg kanala. I pored toga što i u ovom slučaju postoji višestazno prostiranje signala (engl. multipath), kašnjenja komponenata signala u sekundarnim kanalima mnogo su kraća od trajanja čipova, te ne dolazi do izražene međusimbolske interferencije u kanalu. Ovakav kanal se modeluje kao kanal sa ravnim fedingom α_i i Gausovim šumom ξ_{ii} sa srednjom vrednošću nula i varijansom jednakoj snazi šuma. Promene fedinga su spore, tako da se u proseku uzima da je svaki bit pogođen istim koeficijentom Rejljevog fedinga $\alpha = \alpha_{00}$ i da im je srednja snaga koeficijenata jednaka jedinici, tj. $\eta_{\alpha\alpha} = 2b^2 = 1$. U ovom slučaju kanal na slici 1 ima samo jedan množač za feding i jedan sabirač za šum.

Nakon korelacije, slučajni odmerak bita na izlazu korelatora je:

$$z_i^g = \sum_{t=1}^{2\beta} \sum_{n=1}^N \alpha_i x_{ii}^n x_{ii}^g + \sum_{t=1}^{2\beta} \xi_{ii} x_{ii}^g = \sum_{t=1}^{2\beta} \alpha_i (x_{ii}^g)^2 + \sum_{t=1}^{2\beta} \sum_{n=1, n \neq g}^N \alpha_i x_{ii}^n x_{ii}^g + \sum_{t=1}^{2\beta} \xi_{ii} x_{ii}^g$$

što predstavlja slučajnu funkciju za koju se može naći srednja vrednost i varijansa i uvrstiti u opšti izraz za verovatnoću greške bita:

$$p_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{\eta_z^2}{2\sigma_z^2}} \quad (3)$$

čime se dobija izraz za verovatnoću greške bita u zatvorenom obliku

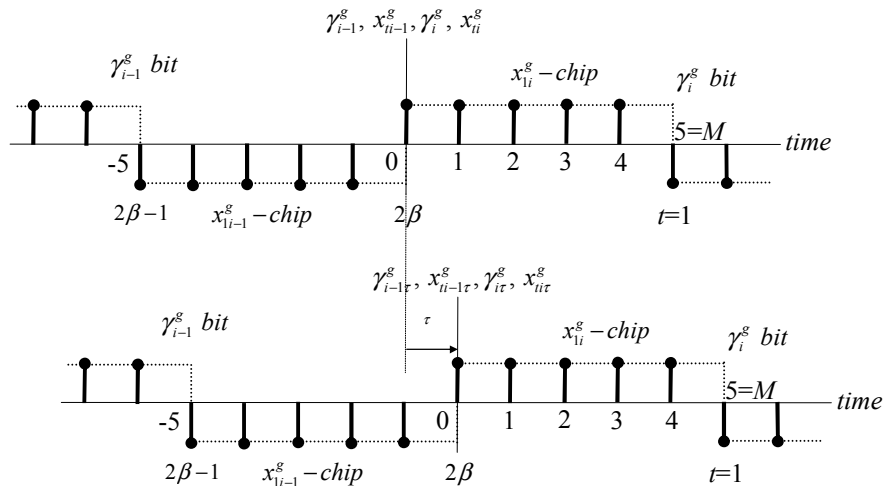
$$p_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{\eta_z^2}{2\sigma_z^2}} = \frac{1}{2} \operatorname{erfc} \left[\frac{2\beta(4-\pi) + 4N - 2}{\beta\pi} + \frac{2}{b^2\pi} \left(\frac{E_b}{N_0} \right)^{-1} \right]^{\frac{1}{2}} \quad (4)$$

gde je 2β procesno pojačanje, srednja snaga fedinga se uzima da je jedan, tj. $2b^2=1$, N je najveći mogući broj učesnika u sistemu, a E_b/N_0 je odnos signala i šuma u sistemu.

Na osnovu izvedenog izraza mogu se doneti sledeći zaključci: kada se povećava broj učesnika N u sistemu povećava se i verovatnoća greške, što je razumljivo, jer u tom slučaju dolazi do povećanja međuučesničke interferencije. U slučaju da se povećava procesno pojačanje 2β dolazi do smanjenja verovatnoće greške, jer se poboljšavaju statističke karakteristike kodne sekvence. Posledica ovog povećanja jeste i povećanje spektra signala.

Teorijski model CDMA sistema sa frekvencijski selektivnim fedingom i širokopojasnim kanalom

Kanal je širokopojasan u slučaju kada frekvencijski opseg signala prelazi koherentni opseg kanala, radi čega kašnjenja komponenta signala u sekundarnim kanalima mogu da budu čak veća od trajanja pojedinog čipa, pa je pojava međusimbolske interferencije značajna i mora se uzeti u obzir pri analizi sistema.



Slika 3 – Prijemne sekvence na izlazu primarnog i sekundarnog kanala.

Indeks τ pokazuje kašnjenje sekvenci

Figure 3 – Received sequences at the output of the primary and secondary channel.

The index τ represents the delay of the sequence

Ovde će se prezentirati slučaj kada u sistemu postoji primarni kanal karakterisan feding koeficientom α_{00} i sekundarni kanal karakterisan kašnjenjem $\tau_j = \tau$ i koeficijentom fedinga α_{01} . U kanalu je prisutan Gausov šum sa varijansom σ_ξ^2 . Za ovaj slučaj, kanal na slici 1 predstavljen je podebljanim linijama. Radi jasnoće objašnjenja rada prijemnika, svaki čip primljenog signala predstavljen je sa M odmeraka jednake amplitude, kao što je prikazano na slici 3 za $M = 5$.

Primljena sekvenca u primarnom kanalu predstavljena je sa nultim kašnjenjem, dok je sekvenca u sekundarnom kanalu prikazana sa kašnjenjem $\tau_j = \tau = 1$. Dakle, usvojena je pretpostavka da su kašnjenja čipova u pojedinim kanalima jednaka delu trajanja čipa τ , što odgovara odzivu kanala gde su pojedini impulsi blizu jedan drugoga i sa vremenskim razmakom manjim od trajanja čipa.

Princip rada prijemnika

U slučaju kada se ne koriste blokovi interlivera (IL) i deinterlivera (DI), koji su prikazani na slici 1, primljeni čip na izlazu iz množača u korelatoru sekvence prijemnika može se predstaviti u ovom vidu

$$E_{corr} = E_{corr}^x + E_{corr}^d + E_{corr}^\xi$$

pri čemu je

$$E_{corr}^x = s\alpha_{00} \sum_{n=1}^N x_{in}^n x_{in}^g + \tau\alpha_{01} \sum_{n=1}^N x_{in}^n x_{in}^g,$$

$$E_{corr}^d = (s - \tau)\alpha_{01} \sum_{n=1}^N x_{in}^n x_{in}^g, \quad i$$

$$E_{corr}^\xi = \xi_{in} x_{in}^g.$$

Nakon obrade u sabiraču korelatora dobija se diskretni odmerak koji sadrži signal, međuučesničku interferenciju, međusimbolsku interferenciju i šum, koji se može predstaviti sledećim izrazom:

$$z_i^g = \sum_{t=1}^{2\beta} \left[s\alpha_{00} + (s - \tau)\alpha_{01} \right] \sum_{n=1}^N x_{in}^n x_{in}^g + \sum_{t=1}^{2\beta} \tau\alpha_{01} \sum_{n=1}^N x_{in}^n x_{in}^g + \sum_{t=1}^{2\beta} s\xi_{in} x_{in}^g = A + B + C \quad (5)$$

Ovaj odmerak predstavlja primljeni bit i dovodi se na ulaz sklopa odluke (SO). Niz ovih odmeraka predstavlja jednu realizaciju stohastičkog procesa u diskretnom vremenu. Izraz (3) realizacija je slučajne varijable Z_i^g koja ima Gausovu distribuciju prema centralnoj graničnoj teoremi (Papoulis, Pillai, 2002), pošto je predstavljena zbirom nezavisnih i identičnih slučajnih varijabli. Radi toga je dovoljno naći srednju vrednost i varijansu ove distribucije, što omogućava da se izvede izraz za verovatnoću greške u sistemu. Srednja vrednost je

$$\eta_z = E\{z_i^g\} = E\{A+B+C\} = E\{Y\} \cdot 2\beta P_c \quad (6)$$

gde je $E\{Y\} = E\{s\alpha_{00} + (s-\tau)\alpha_{01}\}$ i P_c srednja snaga čipova. Zbog statističke nezavisnosti varijabli A, B i C, srednja kvadratna vrednost za z_i^g je $E\{(z_i^g)^2\} = E\{A^2\} + E\{B^2\} + E\{C^2\}$. Navedena matematička očekivanja, zbog statističke nezavisnosti fedinga, kašnjenja, šuma i kodnih sekvenci, mogu se izračunati na sledeći način:

$$E\{A^2\} = 2\beta E\{Y^2\} E\{(z_i^g)^4\} + E\{Y^2\} 2\beta(2\beta-1)P_c^2,$$

$$E\{B^2\} = 2\beta P_c^2 E\{(\alpha_{01}\tau)^2\},$$

$$E\{C^2\} = 2\beta s^2 \sigma^2 P_c.$$

Varijansa se sada može predstaviti u sledećem obliku:

$$\sigma_z^2 = E\{(z_i^g)^2\} - \eta_z^2 = 2\beta E\{Y^2\} E\{(z_i^g)^4\} + E\{Y^2\} 2\beta(2\beta-1)P_c^2 + 2\beta P_c^2 E\{(\alpha_{01}\tau)^2\} + 2\beta s^2 \sigma^2 P_c - (2\beta E\{Y\} P_c)^2 \quad (7)$$

Koristeći relacije (6) i (7), verovatnoća greške bita sada se može naći prema sledećem izrazu:

$$p_e = \frac{1}{2} \operatorname{erfc} \sqrt{\frac{\eta_z^2}{2\sigma_z^2}} = \frac{1}{2} \operatorname{erfc} \left[\frac{E\{Y^2\}}{\beta E\{Y\}} (\Psi + 2\beta + N - 2) - 2 + \frac{E\{(\alpha_{01}\tau)^2\} N}{\beta E\{Y\}} + \frac{s^2}{E\{Y\}} \left(\frac{E_b}{N_0} \right)^{-1} \right]^{\frac{1}{2}} \quad (8)$$

gde je $\Psi = E\{(z_i^g)^4\} / P_c^2$ član koji odražava nebinarnu strukturu haotičnih kodnih sekvenci. Usvaja se pretpostavka da su srednje snage svih čipova međusobno jednake. Uprkos statističkoj strukturi čipova ova pretpostavka je validna, pošto se u ovakvim sistemima prenosa koriste relativno velika procesna pojačanja.

Princip rada prijemnika sa interlivingom

Feding u kanalu degradira prenos digitalnog signala i znatno povećava greške bita na prijamoj strani. Jedna od metoda zaštite prenosa signala u uslovima fedinga je primena interlivinga (Berber, 2008), (Zhan, Berber, 2008). U ovom radu biće analiziran slučaj kada je blok interliving tehnika primenjena u prenosu signala. Dakle, na predajnoj strani je blok intelivera matricne strukture, koji upisuje sve čipove prvog bita u prvi red, a poslednjeg od 2β bita u poslednji red matrice. Zatim se čipovi prvog stupca iščitavaju i prenose u kanalu, a zatim slede i ostali čipovi po stupcima. Na prijamoj strani čipovi se učitavaju u odgovarajuće stupce prijemne matrice, a zatim iščitavaju po redovima, tako da se ponovo formiraju bitovi poslana poruke. Pošto feding u kanalu pogađa bitove sa različitim koeficijentima, primljeni bitovi sadrže čipove koji sadrže različite statistički nezavisne koeficijente fedinga. Radi toga se može očekivati da uticaj fedinga bude umanjen i da se verovatnoća greške poboljšava, tako da teži vrednosti koja se dobija kada je samo šum prisutan u kanalu.

Koristeći identičnu proceduru izvođenja izraza za verovatnoću greške bita, koja je korišćena u slučaju sistema bez interlivinga, diskretni odmerak na izlazu sabirača korelatora je realizacija slučajne funkcije Z_i^g , koji se može izraziti na sledeći način:

$$z_i^g = [2s - \tau] \sum_{t=1}^{2\beta} \sum_{n=1}^N \alpha_t x_{in}^n x_{in}^g + \sum_{t=1}^{2\beta} \omega_{0t} \sum_{n=1}^N x_{tdn}^n x_{in}^g + \sum_{t=1}^{2\beta} s \zeta_{it} x_{in}^g = A + B + C \quad (9)$$

Feding koeficijent označen je indeksom t koji pokazuje redosled čipova u okviru jednog bita, dok indeks d označava kašnjenje čipova. Broj jednakih odmeraka u jednom čipu označen je sa s , a kašnjenje u sekundarnom kanalu sa τ . Odnos s/τ specificira deo vremena za koje signal u sekundarnom kanalu kasni u odnosu na primarni kanal. Srednja vrednost ove slučajne varijable, zbog statističke nezavisnosti slučajnih funkcija A , B i C , jeste:

$$\eta_z = E\{z_i^g\} = E\{A\} + E\{B\} + E\{C\} \quad (10)$$

Pojedinačna očekivanja računaju se na sledeći način. Očekivanje slučajne funkcije A može se predstaviti u ovom vidu:

$$\begin{aligned} E\{A\} &= E\left\{ (2s - \tau) \sum_{t=1}^{2\beta} \sum_{n=1}^N \alpha_t x_{in}^n x_{in}^g \right\} = E\left\{ (2s - \tau) \left[\sum_{t=1}^{2\beta} \alpha_t x_{in}^{g^2} + \sum_{t=1}^{2\beta} \sum_{\substack{n=1 \\ n \neq g}}^N \alpha_t x_{in}^n x_{in}^g \right] \right\} \\ &= E\{(2s - \tau)\} \cdot E\left\{ \sum_{t=1}^{2\beta} \alpha_t x_{in}^{g^2} \right\} + E\{(2s - \tau)\} \cdot E\left\{ \sum_{t=1}^{2\beta} \sum_{n=1, n \neq g}^N \alpha_t x_{in}^n x_{in}^g \right\} \end{aligned}$$

Zbog statističke nezavisnosti slučajnog kašnjenja, fedinga i generisanih haotičnih sekvenci, ovaj izraz može se pojednostaviti, čime se dobija:

$$E\{A\} = E\{(2s - \tau)\} \cdot \sum_{i=1}^{2\beta} E\{\alpha_i\} E\{x_i^{s^2}\} = E\{Y\} \cdot E\{\alpha\} 2\beta P_c = \eta_z$$

gde je $E\{Y\} = E\{2s - \tau\}$ i P_c srednja snaga čipova. Ova srednja vrednost jednaka je srednjoj vrednosti slučajne varijable Z_i^9 , pošto su očekivanja od B i C jednaka nuli. I u ovom slučaju, zbog statističke nezavisnosti varijabli A, B i C, srednja kvadratna vrednost za z_i^9 je $E\{(z_i^s)^2\} = E\{A^2\} + E\{B^2\} + E\{C^2\}$. Navedena matematička očekivanja mogu se izračunati na sledeći način:

$$E\{A^2\} = E\left\{ \left[(2s - \tau) \sum_{i=1}^{2\beta} \sum_{n=1}^N \alpha_i x_{in}^s x_{in}^s \right]^2 \right\}$$

$$= 2\beta P_c^2 E\{Y^2\} \cdot \left[E\{\alpha^2\} E\{(x_i^s)^4\} / P_c^2 + E^2\{\alpha\} (2\beta - 1) + (N - 1) E\{\alpha^2\} \right]$$

$$E\{B^2\} = 2\beta N P_c^2 E\{\tau^2\} E\{\alpha^2\}, \text{ i}$$

$$E\{C^2\} = 2\beta s^2 \sigma^2 P_c.$$

Varijansa se sada može izračunati na sledeći način:

$$\sigma_z^2 = E\{(z_i^s)^2\} - \eta_z^2$$

$$+ 2\beta P_c^2 E\{Y^2\} \cdot \left[E\{\alpha^2\} E\{(x_i^s)^4\} / P_c^2 + E^2\{\alpha\} (2\beta - 1) + (N - 1) E\{\alpha^2\} \right] \quad (11)$$

$$+ 2\beta N P_c^2 E\{\tau^2\} E\{\alpha^2\} + 2\beta s^2 \sigma^2 P_c - (2\beta E\{Y\} E\{\alpha\} P_c)^2$$

Izraz (1) može da se pojednostavi i iskoristi da se dobije izraz za verovatnoću greške bita na osnovu izraza (3), (10) i (11) u ovom vidu

$$p_e = \frac{1}{2} \operatorname{erfc} \left[\frac{4E\{Y^2\}}{\beta\pi E^2\{Y\}} \cdot \left(\Psi + \frac{\pi(2\beta - 1)}{4} + N - 1 \right) - 2 + \frac{4E\{\tau^2\}N}{\beta\pi E^2\{Y\}} + \frac{2s^2}{\pi b^2 E^2\{Y\}} \left(\frac{E_b}{N_0} \right)^{-1} \right]^{-1/2} \quad (12)$$

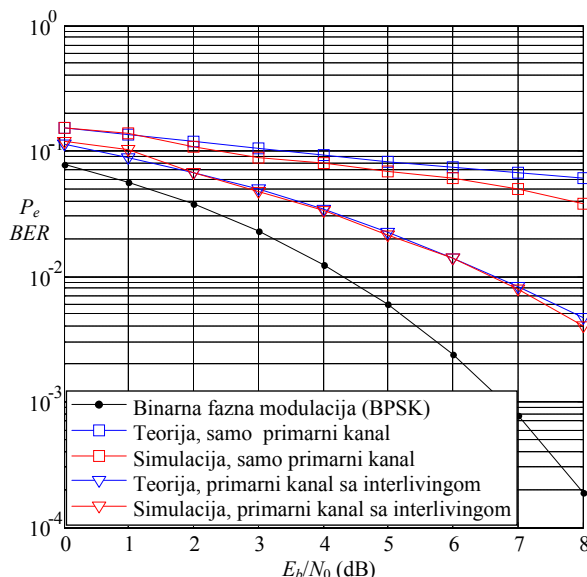
gde je $\Psi = E\{(x_i^s)^4\} / P_c^2$ član koji odražava nebinarnu strukturu haotičnih kodnih sekvenci i $Y = 2s - \tau$.

Simulacioni model CDMA sistema i rezultati simulacije

Sistem prikazan na slici 1, koji je matematički modelovan u prethodnom poglavlju, simuliran je u Matlabu. Simulator je izrađen tako da omogućava promene parametara sistema, kao i detaljno ispitivanje njegovih karakteristika. Generisane su krive učestanosti grešaka bita (engl. bit error rate, BER) i upoređivane sa teorijskim krivama za verovatnoću greške bita P_e definisane relacijama (4), (8) i (12). Naporedo sa ovim grafovima za CDMA sistem prikazani su i grafovi za verovatnoću greške bita u sistemu sa binarnom digitalnom faznom modulacijom (engl. binary phase shift keying, BPSK) radi upoređenja ova dva sistema, pri čemu su dijagrami za binarnu faznu modulaciju korišćeni kao reference.

Simulacija sistema sa uskopojasnim kanalom i ravnim fadingom

Na slici 4 prikazani su grafovi dobijeni simulacijom uskopojasnog sistema naporedo sa teorijskim grafovima dobijenim na osnovu izraza (4), za slučaj kada je procesno pojačanje $2\beta = 100$ i $N = 4$ korisnika aktivno u sistemu, dok je blok interlivinga definisan matricom dimenzija $2\beta \times 2\beta$. Zbog uticaja međuučesničke interferencije, verovatnoća greške u CDMA sistemu je veća od verovatnoće greške koja bi se dobila u binarnom sistemu.



Slika 4 – Verovatnoća greške bita kao funkcija odnosa signal – šum u slučaju kada postoji samo primarni kanal sa ravnim fadingom, za $N = 4$ ušesnika i procesnim pojačanjem $2\beta = 100$
Figure 4 – Probability of error as a function of the signal to noise ratio in the case when only the primary channel with flat fading exists, for $N = 4$ users and the processing gain $2\beta = 100$

Teorijske krive, u slučaju prisustva fedinga, veoma su blizu simulacionim krivama (gornja dva grafa). Razlika u položaju krivih može se objasniti usvojenim pretpostavkama da je distribucija slučajnog odmerka na ulazu u sklop odluke (SO) aproksimirana Gausovom distribucijom u svim teorijskim razmatranjima.

U slučaju korišćenja interlivinga ove krive se spuštaju niže (smanjuje se verovatnoća greške bita) težeći krivoj definisanoj prisustvom isključivo šuma u kanalu, kao što se i vidi na slici 4. U ovom slučaju su teorijska i simulaciona kriva skoro identične. Razlog tome je činjenica da je postupkom interlivinga uticaj fedinga „slučajno raspoređen u prijemnom signalu“, te je simulacija veoma bliza teoriji.

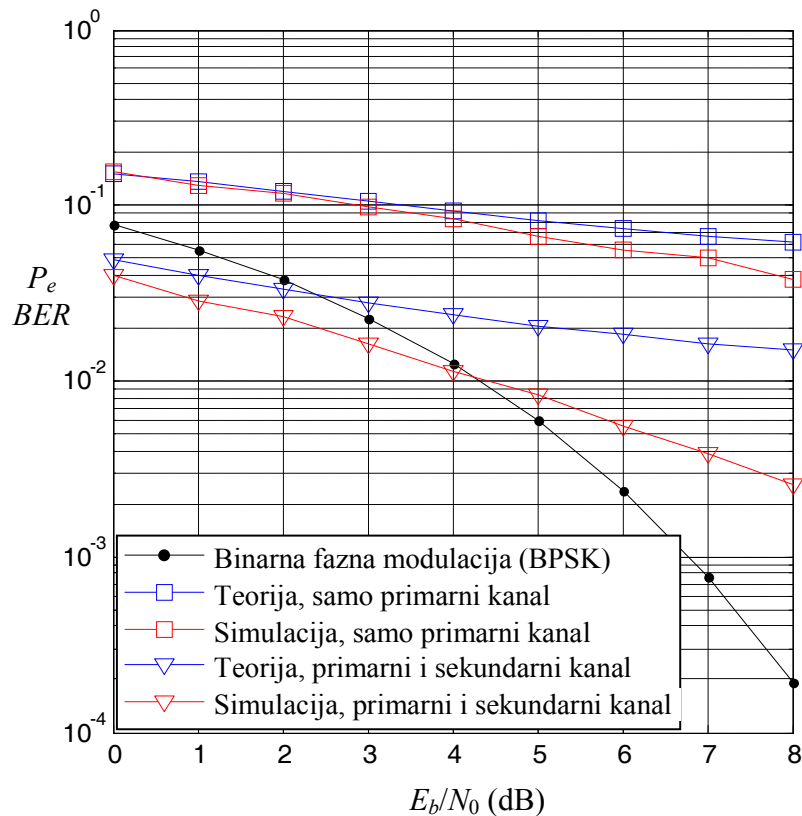
Verovatnoća greške u ovom sistemu može se smanjiti povećanjem procesnog pojačanja. Negativna posledica ovog postupka jeste da se povećava frekvencijski opseg predajnog signala, što se u svakom slučaju želi izbeći. Do ovog smanjenja verovatnoće greške dolazi radi smanjenja međuučesničke interferencije. Naime kada se poveća broj čipova u datom bitu, unakrsna korelacija učesničkih sekvenci se smanjuje, a autokorelacija date učesničke sekvence se povećava.

Postoji još jedna prednost uzrokovana povećanjem procesnog pojačanja. Tajnost prenosa i zaštita od presretanja korisničke informacije se povećava, jer predajni signal postaje „više“ slučajan i, samim tim, sličniji šumu u kanalu.

Simulacija sistema sa širokopojasnim kanalom i frekvencijski selektivnim fedingom bez interlivinga

Na slici 5 prikazani su grafovi za verovatnoću greške u slučaju kada je frekvencijski selektivni feding prisutan u kanalu, koji su dobijeni na osnovu izraza (8). Radi komparacije dodati su grafovi dobijeni u kanalu sa ravnim fedingom (gornji grafovi).

U ovom slučaju mora se dodati uticaj sekundarnog kanala na karakteristike prijemnog signala. Kašnjenje signala sekundarnog kanala izraženo je u diskretnim jednicama i označeno sa τ kao i u teorijskoj analizi. Simulirani broj identičnih odmeraka u jednom čipu bio je 40 dok je srednja vrednost kašnjenja definisana da bude $\tau = 5$, što znači da se približno 80% zakašnjenog čipa u sekundarnom kanalu nalazi unutar trajanja odgovarajućeg čipa u primarnom kanalu. Radi konstruktivnog dodavanja signala iz sekundarnog kanala, verovatnoća greške bita je manja nego u slučaju kada se prima samo signal iz primarnog kanala. Tako se za odnos signal i šum od 8 dB, teorijska verovatnoća greške smanji sa 6×10^{-2} na verovatnoću greške $1,3 \times 10^{-2}$, dok se greška u simulacionom sistemu smanji sa 4×10^{-2} na vrednost $2,3 \times 10^{-3}$.



Slika 5 – Grafovi zavisnosti verovatnoće greške od odnosa signal–šum u kanalu sa ravnim fedingom i sa frekvencijski selektivnim fedingom, za 4 korisnika, procesno pojačanje $2\beta = 100$ i srednju vrednost kašnjenja $\tau = 5$

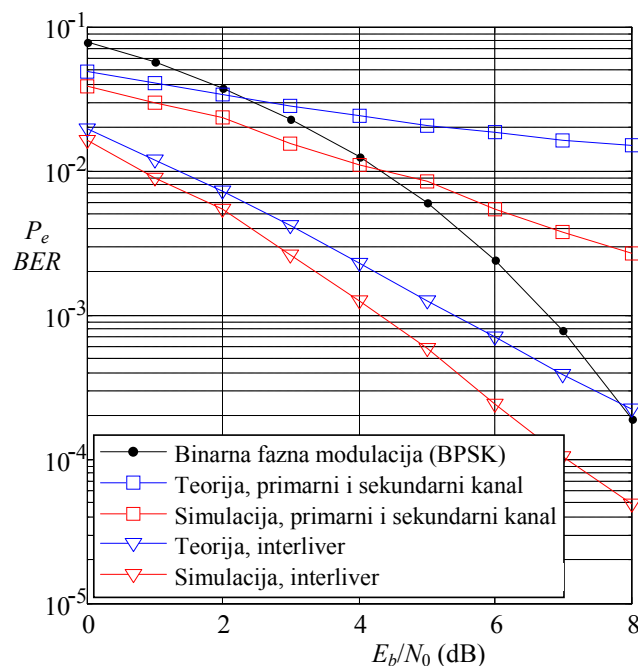
Figure 5 – Graphs of the probability of error as a function of the signal to noise ratio in the channel with both flat fading and frequency selective fading, for 4 users, the processing gain $2\beta = 100$ and the average delay $\tau = 5$

Pokazuje se da je očekivana greška dobijena simulacijom znatno manja od greške koja se očekuje prema teorijskom izrazu. Razlog za to treba tražiti u načinu generisanja kašnjenja u sistemu. Naime, teorijski model uključuje srednju vrednost kašnjenja. U simulaciji, u skladu sa funkcijom gustine verovatnoće kašnjenja, mnogo češće se generišu kašnjenja manja od srednje vrednosti. Samim tim, i očekivana verovatnoća greške dobijena simulacijom je manja. Dakle, u analizi ovih sistema potrebno je uvek imati na umu pretpostavke uzete u toku teorijske analize i procedure koje su korišćene za generisanje signala u toku simulacije.

Simulacija sistema sa širokopoljaskim kanalom i frekvencijski selektivnim fedingom sa interlivingom

Interliving tehnika koristi se da se smanji uticaj feding u sistemu. Teorijski grafovi, koji su dobijena na osnovu izraza (12), i grafovi dobijeni simulacijom prikazani su na slici 6. Smanjenje greške bita u ovom slučaju slično je odgovarajućem smanjenju dobijenom u sistemu sa ravnim fedingom koji je predstavljan samo sa primarnim kanalom.

Zbog konstruktivnog kombinovanja signala u prijemu, krive na slici 6 padaju ispod krive za binarnu faznu modulaciju (BPSK). Dva razloga su uzrokovala ovakvo ponašanje sistema. Prvo, uticaj fedinga je interlivingom dekorelisan, te se feding ponaša kao šum u sistemu. Drugo, signal iz sekundarnog kanala doprinosi snazi signala iz primarnog kanala, te se ukupna snaga prijemnog signala povećava. Time, za istu snagu šuma, raste odnos signala i šuma i pada verovatnoća greške. Primenom interlivinga smanjuje se razlika između teorijske i simulirane krive u odnosu na istu razliku u sistemu bez interlivinga, što je posledica dekorelacije uticaja fedinga u sistemu.



Slika 6 – Grafovi zavisnosti verovatnoće greške od odnosa signal–šum u kanalu sa frekvencijski selektivnim fedingom u sistemu sa i bez interlivinga, za 4 korisnika, procesno pojačanje $2\beta = 100$ i srednju vrednost kašnjenja $\tau = 5$

Figure 6 – Graphs of the probability of error as a function of the signal to noise ratio in the channel with frequency selective fading, for 4 users, the processing gain $2\beta = 100$ and the average delay $\tau = 5$

Zaključak

Osnovni cilj istraživanja, čiji rezultati su prikazani u ovom članku, jeste da se ispituju karakteristike CDMA sistema u uslovima postojanja frekvencijski selektivnog fadinga u širokopojasnom kanalu prenosa signala. Izrađen je i prikazan teorijski model ovog sistema i izvedeni izrazi za verovatnoću greške bita u zatvorenom vidu. Posebno je analiziran slučaj kada je u sistemu primenjena tehnika blok interleavinga. Izvedeni teorijski izrazi za verovatnoću greške bita pokazuju da je moguće ostvariti znatno poboljšanje kvaliteta prenosa signala korišćenjem ove tehnike. Zahvaljujući slučajnoj prirodi haotičnih sekvenci, tajnost u prenosu informacionog sadržaja je povećana. Zbog istog razloga ostvarena je i zaštita sistema od presretanja. Modelovani sistem je simuliran u matlabu. Rezultati simulacije potvrdili su rezultate teorijske analize.

Literatura

Balakrishnan K., Cassioli D., Chong C-C., Emami S., Fort A., Karedal J., Kunisch J., Schantz H., Schuster U., Siwiak K., 2006, IEEE 802.15.4a channel model – final report, (<http://www.ieee802.org/15/pub/04/15-04-0662-02-004a-channel-model-final-report-r1.pdf>).

Berber S., 2006, A Noise Phase Shift Keying for Secure Multiuser Code Division Multiple Access Systems, MILCOM, Washington, 23-25 Oct., Paper 1856, pp.1 – 6.

Berber S., Jovic B., 2006, Sequence synchronization in a wideband CDMA system, in Proceedings of the 2006 International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless06), Sydney, Australia, pp.1–6.

Berber S., 2008, Fading Mitigation in an Interleaved Noise-Based DS-CDMA System for Secure Communications, The Fifth IASTED Int. Conf. on Sign. Proc., Pattern Rec., and Applications, SPPRA 2008, Innsbruck, Austria, February 13 – 15, pp. 260-265.

Berber S., Feng S., 2013, Chaos-Based Physical Layer Design for WSN Applications, 17th WSEAS Int. Conf. on Communications, Rhodes, Greece, July 16-19, pp.157-162.

Brennan D.G., 1959, Linear Diversity Combining Techniques, *Proceedings of IRE*, vol. 47, pp.1075-1102.

Chen L-M., i Chen B-S., 2001, A robust Adaptive DFE Receiver for DS-CDMA System under Multipath Fading Channel, *IEEE Trans. on Signal Processing*, vol. 49, no. 7, pp.1523–1532.

Cimatti G., Rovatti R. i Setti, G., 2007, Chaos-Based Spreading in DS-UWB Sensor Networks Increases Available Bit Rate, *IEEE Trans. Circuits Syst. I*, vol. 54, no. 6, pp. 1327-1339.

Heidari-Bateni G., McGillem C. D., 1994, A chaotic direct-sequence spread-spectrum communication system, *IEEE Trans. on Comm.*, vol. 42, no. 234, pp.1524–1527.

Jovic B., Berber S., Unsworth C.P., 2006, A novel mathematical analysis to predict master-slave synchronization for the simplest quadratic chaotic flow, Ueda chaotic system and the two-well potential Duffing-Holmes oscillator, *Physica D*, vol. 213, Issue 1, pp.31 – 50.

Jovic B., Unsworth C., Sandhu G., Berber S., 2007, A robust sequence synchronization unit for multi-user DS-CDMA chaos-based communication systems, *Signal Processing*, vol. 87, no. 7, pp.1692 – 1708.

Kaddoum G., Roviras D., Charge P., Fournier-Prunaret D., 2009a, Robust synchronization for asynchronous multi-user chaos-based DS-CDMA, *Signal Processing*, vol. 89, no. 5, pp.807 – 818.

Kaddoum G., Roviras D., Chargé P., Fournier-Prunaret D., 2009b, Accurate bit error rate calculation for asynchronous chaos-based DS-CDMA over multipath channel, *Eurasip Journal on Advances in Signal Processing*, Article number 571307.

Kaddoum G., Chargé P., Roviras D., Fournier-Prunaret D., 2009c, A methodology for bit error rate prediction in chaos-based communication systems, *Springer, Birkhäuser Circuits Systems and Signal Processing*, Vol. 28, pp.925-944.

Kaddoum G., Chargé P., Roviras D., 2009d, A generalized methodology for bit-error-rate prediction in correlation-based communication schemes using chaos, *IEEE Communication Letters*, Vol. 13, Issue 8, pp.567-569.

Kaddoum G., Coulon M., Roviras D., Chargé P., 2010, Theoretical performance for asynchronous multi-user chaos-based communication systems on fading channels, *Elsevier Sig. Processing*, Vol. 90, Issue 11, pp.2923-2933.

Kaddoum G., Lombard T., Gagnon F., 2012a, Performance analysis of chaos shift keying system with a polarization sensitive under multipath channel, *IET Communications*, Vol. 6 (12), pp 1837-1845.

Kaddoum G., Gagnon F., 2012b, Design of a High-Data-Rate Differential Chaos-Shift Keying System, *IEEE Trans. Circuits Syst. II*, vol. 59, no. 7, pp.448-452.

Kaddoum G., Richardson F-D, Gagnon F., 2013, Design and Analysis of a Multi-Carrier Differential Chaos-Shift Keying Communication System, *IEEE Tr. on Comm.*, vol. 61, no. 8, pp.3281-3291.

Kao J., Berber S. M., Kecman V., 2010, *Blind Multi-User Detector of a Chaos-Based CDMA Using Support Vector Machine*, IEEE Transactions on Neural Networks, Vol. 21, No. 8, pp.1221 – 1231.

Kolumban G., Kennedy M. P., Chua L. O., 1997, The role of synchronization in digital communications using chaos. i. fundamentals of digital communications, *IEEE Trans. Circuits Syst. I*, vol. 44, no. 10, pp.927–936.

Kolumban G., Kennedy M. P., Chua L. O., 1998, The role of synchronization in digital communications using chaos. ii. chaotic modulation and chaotic synchronization, *IEEE Trans. Circuits Syst. I*, vol. 45, no. 11, pp.1129–1140.

Kolumban G., Kennedy M. P., Chua L. O., 2000, The role of synchronization in digital communications using chaos. iii. performance bounds for correlation receivers, *IEEE Trans. Circuits Syst. I*, vol. 47, no. 12, pp.1673–1683.

Kyro, M., et al., 2012, Statistical Channel Models for 60 GHz Radio Propagation in Hospital Environments, *IEEE Transactions on Antennas and Propagation*, 60(3): pp.1569-1577.

Lau F. Tse C., 2004, *Chaos-Based Digital Communication Systems*. Berlin: Springer.

Mazzini G., Setti G., Rovatti R., 1997, Chaotic complex spreading sequences for asynchronous DS-CDMA. I. System modelling and results, *IEEE Tr.. Circ. Syst. I*, vol. 44, no. 10, pp.937–947.

Ochsner H., 1978, Direct-Sequence Spread-Spectrum Receiver for Communication on Frequency-Selective Fading Channels, *IEEE Tr. on Sel. Areas in Comm.*, vol. SAC-5, no. 2, pp.188-193.

Papoulis A, Pillai S. U., 2002, *Probability, Random Variables and Stochastic Processes*, McGraw-Hill Com. Inc., Fourth Edition.

Parlitz U., Chua L., Halle K., Kocarev L., Shang A., 1992, Transmission of digital signals by chaotic synchronization. *Intern. Jour. of Bif. & Chaos in Applied Scien. & Eng.*, vol. 2, no. 4, pp.p973 –977.

Qilian, L., 2011, Radar Sensor Wireless Channel Modeling in Foliage Environment: UWB Versus Narrowband, *IEEE Sensors Journal*, 11(6): pp.1448-1457.

Rovatti R., Setti G., Mazzini G., 1998, Chaotic complex spreading sequences for asynchronous DS-CDMA. Part II. Some theoretical performance bounds, *IEEE Trans. Circuits Syst. I*, vol. 45, no. 4, pp.496–506.

Rovatti R., Mazzini G., Setti G., 2001, Enhanced Rake Receivers for Chaos-Based DS-CDMA, *IEEE Tran. Circuits Syst. I*, vol. 48, no. 7, pp.818–829.

Rovatti R., Mazzini G., Setti G., 2001, Chaos-Based Asynchronous DS-CDMA Systems and Enhanced Rake Receivers: Measuring the Improvements, *IEEE Trans. Cir. Syst. I*, vol. 48, no. 12, pp.1445–1453.

Saleh A. A. M., R. Valenzuela A., 1987, A Statistical Model for Indoor Multipath Propagation, *IEEE Tran. on Sel. Areas in Comm.*, vol. SAC-5, no. 2, pp.128-137.

Setti G., Rovatti R., Mazzini G., 1999, Synchronization Mechanism and Optimization of Spreading Sequences in Chaos-Based DS-CDMA Systems, *IEICE TRANS. on Fundamentals of Elec., Commun. and Computer Sciences*, vol. E82-A, no. 9, pp.1737–1746.

Tam W., Lau F., Tse C., Lawrance A., 2004, Exact analytical bit error rates for multiple access chaos-based communication systems, *IEEE Trans. Circuits Syst. II*, vol. 51, no. 9, pp.473–481.

Tam W. M., Lau F. C. M., Tse C. K., 2004, A multiple access scheme for chaos-based digital communication systems utilizing transmitted reference, *IEEE Tr. Cir. Syst. I*, vol. 51, no. 9, pp.1868–1878.

Torrieri D., Mukherjee A., and Kwo H.M., 2010, Coded DS-CDMA Systems with Iterative Channel Estimation and no Pilot Symbols, *IEEE Trans. on Wireless Comm.*, vol. 9, no. 6, pp.2012-2021.

Vali R., Berber S., Nguang S. K., 2010, Analysis of a Chaos-based Non-coherent Delay Lock Tracking Loop, International Conference on Communications, Cape Town, pp.1-5.

Vali R., Berber S., Nguang S., 2010, Effect of Rayleigh fading on non-coherent sequence synchronization for multi-user chaos based DS-CDMA, *Signal Processing*, vol. 90, no. 6, pp.1924 – 1939.

Xiao P., and Strom E., 2010, Soft Demodulation for Orthogonal Modulated and Convolutionally Coded DS-CDMA Systems, *IEEE Trans. on Comm.*, vol. 58, no. 3, pp.742–747.

Yue L., Weerasinghe N. S., Han C., Hashimoto T., 2010, Partial Multiuser Detection for CS-CDMA/CP over Multipath Channels, *IEEE Trans. on Comm.*, vol. 58, no. 8, pp.2305–2313.

Yu-Nan L. and Lin D. W., 2003, Multiple Access over Fading Multipath Channels Employing Chip-Interleaving CD-DSS, *IEICE Trans. on Comm.*, Vol. E86-B, No. 1.

Yu-Nan L. and Lin D. W., 2005, Novel analytical results on performance of bit-interleaved and chip-interleaved DS-CDMA with convolutional coding, *IEEE Tran. on Veh. Technology*, Vol. 54, pp.996-1012.

Zhan X., Berber S., 2008, Development of a Reverse Chaos Based CDMA Link and Fading Mitigation, International Symposium on Information Theory and its Applications, ISITA 2008, Auckland, New Zealand, Dec. 7–10, pp.711-716.

THEORETICAL ANALYSIS AND SIMULATION OF A CODE DIVISION MULTIPLE ACCESS SYSTEM (CDMA) FOR SECURE SIGNAL TRANSMISSION IN WIDEBAND CHANNELS

FIELD: Telecommunications, Wireless Communication Systems
ARTICLE TYPE: Original Scientific Paper

Summary:

Chaotic spreading sequences can increase secrecy and resistance to interception in signal transmission. Chaos-based CDMA systems have been well investigated in the case of flat fading and noise presence in the channel. However, these systems operating in wideband channels, characterized by the frequency selective fading and white Gaussian noise, have not been investigated to the level of understanding their practical applications. This paper presents a detailed mathematical model of a CDMA system based on chaotic spreading sequences. In a theoretical analysis, all signals are represented in the discrete time domain. Using the theory of discrete time stochastic processes, the probability of error expressions are derived in a closed form for a multi-user chaos based CDMA system. For the sake of comparison, the expressions for the probability of error are derived separately for narrowband and wideband channels. The application of the system interleaving technique is investigated in particular, which showed that this technique can

substantially improve probability of error in the system. The system is simulated and the findings of the simulation confirmed theoretically expected results. Possible improvements in the probability of bit error due to multipath channel nature, with and without interleavers, are quantified depending on the random delay and the number of users in the system. In the analyzed system, a simplified version of the wideband channel model, proposed for modern wideband wireless networks, is used.

Introduction

Over the past years, the demand for wireless communications has increased substantially due to advancements in mobile communication systems and networks. Following these increasing demands, modern communication systems require the ability to handle a large number of users to process and transmit wideband signals through complex frequency selective channels.

One of the techniques for transmission of multi-user signals is the Code Division Multiple Access (CDMA) technique which allows communications of multiple users in the same communication system. This is achieved in such a way that each user is assigned a unique code sequence, which is used at the receiver side to discover the information dedicated to that user. These systems belong to the group of communication systems for direct sequence spread spectrum systems. Traditionally, CDMA systems use binary orthogonal spreading codes.

In this paper, a mathematical model and simulation of a CDMA system based on the application of non-binary, precisely speaking, chaotic spreading sequences. In their nature, these sequences belong to random sequences with infinite periodicity, and due to that they are appropriate for applications in the systems that provide enhanced security against interception and secrecy in signal transmission.

Numerous papers are dedicated to the development of CDMA systems in flat fading channels. This paper presents the results of these systems analysis for the case when frequency selective fading is present in the channel. In addition, the paper investigates a possibility of using interleaving techniques to mitigate fading in a wideband channel with the frequency selective fading.

Basic structure of a CDMA communication system and its operation

In this paper, a CDMA system block schematic is presented and the function of all blocks is explained. Notation to be used in the paper is introduced. Chaotic sequences are defined and explained in accordance with the method of their generation. A wideband channel with frequency selective fading is defined by its impulse response function.

Theoretical analysis of a CDMA system with flat fading in a narrowband channel

A narrowband channel and flat fading are defined. A mathematical analysis of the system is conducted by presenting the signal expressions at vital points in the transmitter and receiver. The expression of the signal at

the output of the sequence correlator is derived. Then the expression for the probability of bit error is derived in a closed form and discussed from both the number of users and the spreading factor point of view.

Theoretical model of a CDMA sistem with frequency selective fading in a wideband channel

A wideband channel and frequency selective fading are defined. All signals in the system are presented in the discrete time domain. In order to use a finite length of chips, each chip is represented by identical samples. A mathematical analysis of a wideband CDMA system is conducted. The mathematical expressions of the signals at vital points in the transmitter and receiver are presented. The expression for probability of bit error is derived in a closed form. The principles of the transmitter and receiver operations with and without interleavers are separately analyzed.

Simulation model of the CDMA system and the simulation results

The following system simulations are presented in this chapter: simulation of the system with a narrowband channel and flat fading; simulation of the system with a wideband channel and frequency selective fading without interleaving and simulation of the system with a wideband channel and frequency selective fading with interleaving. It was shown that the probability of error curves obtained by the simulation follow the curves obtained by the theoretical analysis.

Conclusion

The basic aim of this research, the results of which are shown in this paper, is to investigate the properties of CDMA systems in the case when frequency selective fading is present in a wideband channel. The developed theoretical model of the system is presented and the expressions of the probability of error are derived in a closed form., The case when the block interleaving technique is applied in the system is analysed in particular. The derived theoretical expressions for the probability of error show that it is possible to achieve significant improvement in the quality of signal transmission using this technique. Due to the random nature of chaotic sequences, the secrecy of information transmission is improved. For the same reason, the system's protection against interception is achieved. The modelled system is simulated in Matlab. The results of the simulation confirmed the results of the theoretical analysis.

Keywords: *chaos-based systems, secure signal transmission, CDMA systems, wideband channels, application of interleaving.*

Datum prijema članka/Paper received on: 10. 02. 2014.

Datum dostavljanja ispravki rukopisa/Manuscript corrections submitted on: 08. 03. 2014.

Datum konačnog prihvatanja članka za objavljivanje/ Paper accepted for publishing on: 10. 03. 2014.