Mr Branislav Todorović,
dipl. inž.

Dr Milan Šunjevarić,
pukovnik, dipl. inž.
Vojnotehnički institut VJ,
Beograd

NOVI METOD PROTIVELEKTRONSKE ZAŠTITE RADIO-VEZA U KANALIMA SA FEDINGOM

UDC: 621.391.7:519.724:623.62

Rezime:

U radu je predložen i analiziran novi metod za protivelektronsku zaštitu radio-veza u kanalima sa fedingom. Metod je zasnovan na dobro poznatoj tehnici frekvencijskog skakanja. Novinu predstavlja algoritam kodne sinhronizacije koji obezbeđuje da generator dugog pseudoslučajnog koda startuje uvek iz drugog početnog stanja. Na taj način izviđanje je znatno otežano, a prisluškivanje praktično onemogućeno. Algoritam koristi skup pasivnih korelatora, demodulator poruke i banku aktivnih korelatora. Srednje vreme uspostavljanja kodne sinhronizacije je relativno kratko, a dobija se visoka pouzdanost odluke. Analiziran je uticaj broja pasivnih i aktivnih korelatora na performanse kodne sinhronizacije.

Ključne reči: telekomunikacije, prenos u proširenom spektru, frekvencijsko skakanje, protivelektronska zaštita.

A NEW ELECTRONIC COUNTER-COUNTERMEASURE METHOD FOR RADIO LINKS IN CHANNELS WITH FADING

Summary:

In this paper we propose and analyze a new electronic counter-countermeasure method for radio links in channels with fading. This method is based on the well known frequency hopping technique. The news is an algorithm of code synchronization which provides that long pseudonoise code generator always starts from the different initial state. In that way, a surveillance becomes more difficult while an eavesdropping becomes practically impossible. This algorithm uses the set of passive correlators, a message demodulator and the bank of active correlators. Mean acquisition time is relatively short and high reliability of decision is obtained. The effect of number of passive and active correlators on code synchronization performances is analyzed.

Key words: telecommunications, spread spectrum transmission, frequency hopping, electronic counter-countermeasures.

Uvod

Radio-prenos sa frekvencijskim skakanjem (FS) široko je korišćen u savremenim telekomunikacijama, pre svega zbog povećane zaštite od izviđanja, ometanja i prisluškivanja u odnosu na klasične tehnike, kao i mogućnosti rada u kodnom multipleksu [1]. Osnovni zadatak prijemnika signala sa

frekvencijskim skakanjem jeste da izvrši skupljanje (despreading) dolazećeg korisnog signala, što se ostvaruje korelisanjem dolazećeg signala sa sinhronizovanim lokalno generisanim pseudoslučajnim (PS) kodom. Proces kodne sinhronizacije sastoji se od dva dela: uspostavljanja kodne sinhronizacije (akvizicije) dolazećeg i lokalno generisanog PS koda, kada se vremenska raz-

lika između njih svodi u opseg manji od trajanja jednog PS simbola (čipa), i održavanja kodne sinhronizacije (praćenje) koja dodatno redukuje vremensku razliku ostalu posle akvizicije.

U tehničkoj literaturi predloženo je i analizirano više metoda za uspostavljanje kodne sinhronizacije. Kodna sinhronizacija kratkih PS kodova može se uspostaviti korišćenjem nekog od algoritama na osnovu serijskog pretraživanja [1, 3]. Ukoliko je interval neodređenosti relativno kratak, tada se i vrlo dugi PS kodovi takođe mogu sinhronizovati korišćenjem nekog od algoritama sa serijskim pretraživanjem [4, 5]. Ukoliko je odnos signal—šum na ulazu prijemnika visok, uspostavljanje sinhronizacije se može ostvariti korišćenjem frekvencijske estimacije [6]. Jedan od mogućih pristupa za uspostavljanje sinhronizacije vrlo dugih PS kodova jeste takozvana sinhronizacija na dva nivoa koja se zasniva na serijskom pretraživanju, a takvo uspostavljanje kodne sinhronizacije za FS signale, koje kombinuje brzinu pretraživanja pasivne korelacije i pouzdanost odluke zasnovanu na integraciji po velikom broju čipova, predloženo je i analizirano u referenci [7]. Ovaj metod koristi jedan pasivni korelator prilagođen na preambulu (nekoliko puta ponovljen kratki PS kod — KPSK). Pošto se uspostavi sinhronizacija preambule, taj korelator generiše startni signal za dugi PS kod (DPSK), a generator DPSK startuje iz prethodno definisanog početnog stanja. Banka aktivnih korelatora koristi se za verifikaciju ispravnih i odbacivanje lažnih startnih signala dugog PS koda. Da bi se izbeglo da DPSK generator startuje uvek iz istog početnog stanja, ono se može menjati u određenim vremenskim intervalima prema odgovarajućem protokolu. Na taj način izviđanje i prisluškivanje su otežani, ali ne i onemogućeni.

Da bi se redukovala verovatnoća nedetekcije signala u uslovima fedinga, metod sa više različitih kratkih PS kodova predložen je u referenci [8]. U referencama [7 i 8] razmatran je slučaj

statičke optimizacije pragova u zavisnosti od nivoa šuma. U referenci [9] opisan je prijemnik koji automatski podešava pragove u zavisnosti od nivoa šuma.

Osnovni nedostatak pomenutih metoda sa preambulom jeste da se kod njih, u određenom vremenskom intervalu, dugi PS kod startuje uvek iz istog početnog stanja. To znači da je isti deo dugog PS koda izložen izviđanju, svaki put kada se sistem koristi za komunikaciju u određenom vremenskom intervalu.

Da bi se prevazišao ovaj problem, u referenci [1] predloženo je i na koncepcijskom nivou razmatrano uspostavljanje kodne sinhronizacije na tri nivoa koje obezbeđuje da DPSK generator startuje uvek iz drugog početnog stanja. Na taj način izviđanje je znatno otežano, a prisluškivanje praktično onemogućeno. Kod kodne sinhronizacije sa tri nivoa akvizicioni proces se realizuje u tri etape. U prvoj etapi pasivni korelator treba da detektuje kratki PS kod. Visok nivo signala na izlazu ovog korelatora aktivira demodulator poruke koji, u drugoj etapi, treba ispravno da demoduliše poruku o početnom stanju generatora dugog PS koda. Po prijemu ove poruke, u trećoj etapi, prijemnik startuje aktivni korelator koji treba da proveri da li je sinhronizacija dugog PS koda uspostavljena ili ne. Analiza ove metode u prisustvu šuma i smetnji data je u referenci [12].

U ovom radu predložena je i analizirana modifikovana kodna sinhronizacija signala sa tri nivoa sa frekvencijskim skakanjem koja je predviđena za rad u prisustvu fedinga. Modifikacija se sastoji u korišćenju više kratkih PS kodova. Modifikovana kodna sinhronizacija koristi skup pasivnih korelatora, demodulator poruke i banku aktivnih korelatora. Pasivni korelatori podešeni su na kratke sinhronoprefikse (kratke PS kodove) kojima je modulisani nosilac. Veći broj pasivnih korelatora smanjuje verovatnoću nedetekcije usled iščezavanja signala u uslovima

fedinga. Ukoliko je prekoračen prag na izlazu bilo kojeg pasivnog korelatora, aktivira se demodulator koji čeka da primi poruku o početnom stanju generatora dugog PS koda. Po prijemu ove poruke aktivira se jedan slobodan aktivni korelator iz banke. Aktivna korelacija se obavlja u dužem intervalu, tako da se dobija visoka pouzdanost odluke.

Model modifikovane kodne sinhronizacije sa tri nivoa

Pretpostavka je da na terenu postoji više mobilnih radio-uređaja koji komuniciraju u push-to-talk režimu. Komunikacije između učesnika održavaju se povremeno, sa prekidima različitog trajanja. Zbog toga je uspostavljanje kodne sinhronizacije od izuzetnog značaja pri projektovanju radio-uređaja sa frekvencijskim skakanjem. Učesnici, a priori, raspolažu informacijom o tome koji dugi PS kod je korišćen, ali ne znaju kada će veza otpočeti pa se mora najpre izvršiti određivanje tog trenutka.

Predajnik — na početku veze između dva učesnika, pozivajuća stanica počinje prenos emitovanjem slučajnog startnog signala koji prekida radio-ćutanje. Za vreme emitovanja ovog signala, koje traje veoma kratko, po-

dešavaju se izlazna kola predajnika. Odmah zatim predajnik emituje uvodnik poruke koji je prikazan na slici 1.

Uvodnik poruke sastoji se od tri dela (nivoa): preambule, poruke o početnom stanju generatora dugog PS koda i segmenta dugog PS koda koji služi za proveru sinhronizacije.

Preambula se sastoji od N_{pc} kratkih PS kodova (sinhroprefiksa). Svaki od njih je dug m čipova, a rastojanje između početaka uzastopnih prefiksa je l čipova. Ukupno vremensko rastojanje između početaka uzastopnih prefiksa je $T_1 = lT_p$, gde je T_p označeno trajanje čipa kratkog PS koda. Dakle, ukupna dužina preambule je $L = N_{pc}l$, a ukupno trajanje preambule je $T_1 = N_{pc}T_l$. Analiza se vrši pod pretpostavkom da je ukupna dužina preambule L konstantna, pri čemu se menja rastojanje l između početaka dva sukcesivna sinhroprefiksa sa promenom broja sinhroprefiksa N_{pc} .

Poruka o početnom stanju generatora dugog PS koda sastoji se od N_2 bita. Ova poruka moduliše poslednji kratki PS kod koji služi kao podnosi-lac. Trajanje drugog nivoa sinhronizacije iznosi $T_2 = N_2T_b$, gde T_b označava trajanje bita.

Dugi PS kod počinje da se emituje čim se prenese poruka o njegovom početnom stanju. Provera ispravnosti ko-

Sl. 1 — Struktura uvodnika poruke

dne sinhronizacije obavlja se za vreme trajanja k čipova dugog PS koda. Trajanje trećeg nivoa sinhronizacije je $T_3 = kT_c$, gde je sa T_c označeno trajanje čipa dugog PS koda.

Po završetku emitovanja uvodnika poruke, predajnik započinje prenos poruke.

Prijemnik — kod modifikovane kodne sinhronizacije sa tri nivoa, prijemnik sadrži tri osnovna dela: skup od N_{pc} pasivnih korelatora, demodulator poruke i banku od N_{ac} aktivnih korelatora. Struktura prijemnika prikazana je na slici 2.

Dolazeći signal prolazi kroz liniju za kašnjenje dužine N_{pc} , pri čemu je razmak između susednih ćelija jednak i iznosi l čipova. Na taj način obezbeđeno je da svi sinhro-prefiksi istovremeno dolaze na odgovarajući pasivni korelator. Ukupno kašnjenje ove linije je $(N_{pc} - 1)lT_p$.

Skup pasivnih korelatora vrši detekciju preambule. Svaki pasivni korelator $(1, 2, \dots, N_{pc})$ podešen je na odgovarajući sinhroprefiks $(1, 2, \dots, N_{pc})$. Pasivni korelatori integrale unutar kliznog prozora širine mT_p . Analiza se obavlja pod pretpostavkom da se odlu-

ka o prisustvu sinhroprefiksa donosi brzinom skakanja preambule, tj. svakih T_p sekundi.

Svaki pasivni korelator označen je svojim identifikacionim brojem koji predstavlja redni broj sinhroprefiksa na koji je podešen. Kada izlaz bilo kog pasivnog korelatora premaši prag t_{pc} , generiše se startni signal demodulatora poruke zajedno sa identifikacionim brojevima odgovarajućih korelatora.

Podatak o identifikacionim brojevima pasivnih korelatora, koji se šalje zajedno sa startnim signalom demodulatora poruke, služi da se usaglase kašnjenja i da se demodulator poruke aktivira po završetku preambule. Po prijemu poruke o početnom stanju DPSK generatora, prijemnik startuje aktivni korelator dužine k skokova ($k \gg m$), koji proverava da li je kodna sinhronizacija uspostavljena ili ne. Na kraju intervala korelacije dugog PS koda, koji traje k skokova, izlaz aktivnog korelatora se upoređuje sa pragom t_{ac} . Ukoliko je ovaj prag premašen, proces uspostavljanja kodne sinhronizacije je završen i prijemnik prelazi u režim praćenja kodne sinhronizacije.

Ukoliko dođe do nekoliko uzastopnih lažnih aktiviranja izlaza pasivnih korelatora može se dogoditi da nekoli-

Sl. 2 — Prijemni deo sklopa za kodnu sinhronizaciju

ko aktivnih korelatora istovremeno integrirali repliku od k skokova dugog PS koda. Startni signali dugog PS koda koji su generisani u trenutku kada su svi aktivni korelatori zauzeti bivaju ignorisani. Verovatnoća da startni signal dugog PS koda dođe na ulaz banke aktivnih korelatora kada su svi aktivni korelatori zauzeti (blokirani), naziva se verovatnoća blokiranja.

Prema tome, kodna sinhronizacija je uspostavljena ukoliko prijemnik detektuje bar jedan od kratkih sinhroprefiksa, ispravno demoduliše poruku o početnom stanju generatora dugog PS koda, startni signal generatora dugog PS koda pronade bar jedan slobodan aktivni korelator i rezultat provere potvrdi da je kodna sinhronizacija uspostavljena.

Odluka o tome da li je sinhronizacija (sinhroprefiksa ili dugog PS koda) uspostavljena donosi se na osnovu rezultata upoređenja nivoa signala na izlazu korelatora (pasivnog ili aktivnog) sa odgovarajućim pragom. Rezultat upoređenja nivoa signala na izlazu korelatora (pasivnog ili aktivnog) sa pragom može se opisati u probabilističkom smislu preko verovatnoće lažnog alarma (P_{fa}) i verovatnoće nedetekcije (P_{fd}):

— verovatnoća lažnog alarma predstavlja verovatnoću da korelator pogrešno detektuje sinhrostanje kada ono ne postoji,

— verovatnoća nedetekcije predstavlja verovatnoću da korelator ne detektuje sinhrostanje kada ono postoji.

Neka je $P_{fa1}(i)$ verovatnoća lažnog alarma na i -tom pasivnom korelatoru, a P_{fa2} verovatnoća lažnog alarma na posmatranom aktivnom korelatoru. Verovatnoće nedetekcije na izlazu i -log pasivnog i aktivnog korelatora označavaju se sa $P_{fd1}(i)$ i P_{fd2} , respektivno.

U prvom nivou uspostavljanja sinhronizacije potrebno je izvršiti detekciju preambule, za šta se koristi skup pasivnih korelatora. Upoređenje signala na izlazu pasivnog korelatora sa pra-

gom vrši se svakih T_p/N sekundi, pri čemu je sa T_p označeno trajanje čipa preambule, a sa N broj upoređivanja po čipu. Kada preambula nije prisutna, signali koji pogrešno indiciraju sinhronizaciju preambule generišu se prosečnom brzinom:

$$\lambda = P_{fa1} R_p, \quad (1)$$

gde je $R_p = N/T_p$ brzina odlučivanja na izlazu pasivnog korelatora koji vrši detekciju preambule. S obzirom na to da se najčešće vrši jedno odlučivanje po čipu, onda je $R_p = 1/T_p$.

U svakom trenutku odlučivanja, do aktiviranja demodulatora poruke i generisanja lažnog startnog signala dugog PS koda može doći ukoliko bar jedan od N_{pc} pasivnih korelatora generiše lažni alarm.

U drugom nivou uspostavljanja sinhronizacije predajnik emituje poruku o početnom stanju generatora dugog PS koda. Ova poruka sastoji se od N_2 bita. Verovatnoća da je svih N_2 bita ispravno primljeno iznosi:

$$P_m = P_b^{N_2} \quad (2)$$

gde P_b predstavlja verovatnoću da je bit ispravno prenet. Ova verovatnoća zavisi od tipa primenjene modulacije — demodulacije, odnosa signal-šum na ulazu prijemnika i vrste zaštitnog kodiranja.

U trećem nivou aktivni korelator dugog PS koda je aktiviran u intervalu kT_c sekundi za koje vreme se vrši provera sinhronizacije.

Pod pretpostavkom da lažni startni signali dugog PS koda stižu približno po Poasonovom zakonu sa brzinom pojavljivanja λ , primenom teorije čekanja aktivnost banke aktivnih korelatora može se modelovati kao sistem sa čekanjem [7] koji ima konačan broj servera — aktivnih korelatora N_{ac} , fiksnim vremenom držanja kT_c i bez vremena za čekanje. U tom slučaju se opterećenje banke aktivnih korelatora može opisati relacijom:

$$a = \lambda kT_c, \quad (3)$$

gde je sa λ označena brzina kojom skup pasivnih korelatora generiše lažne startne signale dugog PS koda. Ovaj parametar može se izračunati na sledeći način [8]:

$$\lambda = \frac{\left[1 - \prod_{i=1}^{N_{pc}} (1 - P_{fal}(i)) \right]}{T_p} \quad (4)$$

Verovatnoća da će startni signal dugog PS koda zateći sve aktivne korelatore iz zauzete (blokirane) banke, naziva se verovatnoćom blokiranja. Ukoliko se banka aktivnih korelatora modeluje na ovaj način, verovatnoća blokiranja može se izračunati preko Erlang-B formule [8]:

$$B(N_{ac}, a) = \frac{\left[\frac{a^{N_{ac}}}{N_{ac}!} \right]}{\sum_{j=0}^{N_{ac}} \left(\frac{a_j}{j!} \right)} \quad N_{ac} = 1, 2, \dots \quad (5)$$

Verovatnoća lažnog hvatanja

Pod lažnim hvatanjem podrazumeva se situacija kada upravljačka jedinica daje signal da je kodna sinhronizacija uspostavljena, a u stvarnosti to nije slučaj. To se događa ukoliko se zastopno dese sledeća tri događaja:

— na izlazu bar jednog od N_{pc} pasivnih korelatora došlo je do pojave lažnog alarma, koji je aktivirao demodulator, posle čega je došlo do generisanja startnog signala dugog PS koda;

— bar jedan od N_{ac} aktivnih korelatora je slobodan, tako da startni signal dugog PS koda nije blokirao;

— aktivni korelator koji je aktiviran startnim signalom dugog PS koda generisao je lažni alarm.

Prema tome, pod pretpostavkom da se startni signali dugog PS koda generišu po Poasonovom zakonu, verovatnoća lažnog hvatanja može se opisati relacijom:

$$P_{fl} = \left[1 - \prod_{i=1}^{N_{pc}} (1 - P_{fal}(i)) \right] \left[1 - B(N_{ac}, a) \right] P_{fa2}. \quad (6)$$

Verovatnoća nedetekcije

Pod nedetekcijom se podrazumeva situacija kada upravljačka jedinica daje signal da kodna sinhronizacija nije uspostavljena, a u stvarnosti jeste. Sinhrostanje neće biti detektovano ako se dogodi bilo koji od sledećih međusobno isključivih događaja:

— nijedan od N_{pc} pasivnih korelatora nije detektovao sinhronizaciju preambule;

— bar jedan pasivni korelator je detektovao sinhronizaciju preambule, ali je pogrešno prenet najmanje jedan od N_2 bita koji sadrže poruku o početnom stanju generatora dugog PS koda;

— bar jedan pasivni korelator je detektovao sinhronizaciju preambule, ispravno je preneto svih N_2 bita, ali su zauzeti svi aktivni korelatori, tako da je startni signal dugog PS koda ignorisan;

— bar jedan pasivni korelator je detektovao sinhronizaciju preambule, ispravno je preneto svih N_2 bita, najmanje jedan aktivni korelator je slobodan, ali nivo signala na izlazu aktivnog korelatora nije premašio prag t_{ac} .

Prema tome, verovatnoća nedetekcije sinhronizacije može se izraziti kao:

$$P_{miss} = \prod_{i=1}^{N_{pc}} P_{fd1}(i) + \left[1 - \prod_{i=1}^{N_{pc}} P_{fd1}(i) \right] (1 - P_m) + \left[1 - \prod_{i=1}^{N_{pc}} P_{fd1}(i) \right] P_m B(N_{ac}, a) + \left[1 - \prod_{i=1}^{N_{pc}} P_{fd1}(i) \right] P_m [1 - B(N_{ac}, a)] P_{fd2}. \quad (7)$$

Problem optimizacije

Verovatnoća lažnog hvatanja i verovatnoća nedetekcije su funkcije praga pasivnih i aktivnih korelatora, parametara sistema i karakteristika kanala. Za dati skup parametara sistema

i karakteristika kanala, relacije (6 i 7) zavise samo od pragova. Funkcionalno, one su oblika:

$$P_{fl} = f(t_{pc}, t_{ac}), \quad (8)$$

$$P_{miss} = f(t_{pc}, t_{ac}). \quad (9)$$

Optimizacija pragova podrazumeva minimiziranje verovatnoće nedetekcije, pri čemu se verovatnoća lažnog hvatanja specificira. Matematički, problem se svodi na iznalaženje pragova t_{pc} i t_{ac} tako da se dobije minimalna verovatnoća P_{miss} pod uslovom da je $P_{fl} \leq 10^{-p}$, gde je $p > 0$.

Model fedinga

Za opisivanje fedinga u radio-kanalu korišćen je Gilbertov model [14]. To je Markovljev model sa dva stanja za kanale sa memorijom. Ova dva stanja su stanje bez fedinga koje se označava sa G (good — dobar) i stanje sa fedingom koje se označava sa B (bad — loš, rđav). Gilbertov model, sa odgovarajućim verovatnoćama prelaza između stanja, prikazan je na slici 3.

Sl. 3 — Gilbertov model fedinga

Model je veoma jednostavan i zbog toga često korišćen. On je konceptijski dobar zbog svoje osobine da generiše greške u paketu, ali ima određenih ograničenja u predstavljanju realnih kanala. Ova ograničenja su posledica njegove regenerativne strukture (renewal nature) i pretpostavke da dužina oba stanja ima geometrijsku raspodelu. Ograničenja se mogu prevazići korišćenjem složenijih modela koji sadrže veći broj stanja sa odgovarajućim verovatnoćama prelaza. Procedure za izračunavanje mera performansi, kao što su verovatnoća lažnog hvatanja i vero-

vatnoća nedetekcije ostaju iste, ali zahtevana kompleksnost izračunavanja i broj parametara rastu sa porastom broja stanja.

Polazna pretpostavka je da kanal ostaje u istom stanju tokom intervala skoka i da se prelazi između stanja mogu događati samo na kraju intervala skoka. S obzirom na to da je trajanje intervala skoka tipično reda 1ms, ova pretpostavka može se smatrati opravdanom.

Dobro i loše stanje se naizmenično smenjuju. Neka su verovatnoće prelaza iz dobrog u dobro, dobrog u loše, lošeg u loše i lošeg u dobro stanje označene sa P_{gg} , P_{gb} , P_{bb} , i P_{bg} , respektivno. Osobina Gilbertovog modela je da trajanje stanja (dobrog ili lošeg) ima geometrijsku raspodelu. To znači da je srednje trajanje fedinga (u skokovima):

$$D = \frac{1}{P_{bg}} \quad (10)$$

Verovatnoća da je kanal pod fedingom predstavlja relativni deo vremena u kojem je kanal pod fedingom. Primenom Gilbertovog modela fedinga ona se može izračunati na sledeći način:

$$F = \frac{P_{gb}}{P_{gb} + P_{bg}} \quad (11)$$

Neka je $P_G(i)$ verovatnoća da kanal nije pod fedingom na početku i -tog sinhroprefiksa i neka je $P_B(i)$ verovatnoća da je kanal pod fedingom na početku i -tog sinhroprefiksa. Razlika između početaka i -tog i $(i+1)$ -og sinhroprefiksa je 1 skokova. Otuda je:

$$[P_G(i+1) \ P_B(i+1)] = [P_G(i) \ P_B(i)] [A]^1 \quad (12)$$

gde je A matrica prelaza definisana sa:

$$A = \begin{pmatrix} P_{gg} & P_{gb} \\ P_{bg} & P_{bb} \end{pmatrix} \quad (13)$$

Izračunavanje matrice A može se uprostiti. Matrica A može se rastaviti tako da je $A = BCB^{-1}$, gde je C dijago-

nalna matrica sopstvenih vrednosti λ_1 i λ_2 matrice prelaza A, dok je B redukciona matrica koja se sastoji od odgovarajućih sopstvenih vektora matrice A, gde su sopstveni vektori napisani kao kolone [16]. Tako je $A^1 = BC^1B^{-1}$, a matrica C je:

$$C^1 = \begin{pmatrix} \lambda_1^1 & 0 \\ 0 & \lambda_2^1 \end{pmatrix} \quad (14)$$

Verovatnoće stanja kanala na početku i-tog sinhroprefiksa mogu se izračunati korišćenjem jednačina (12 i 14). Kanal ima memoriju i generalno teži da ostane u stanju u kojem već jeste. Ova osobina dozvoljava jednostavnu aproksimaciju koja olakšava izračunavanje verovatnoće nedetekcije za dati kratki sinhroprefiks od m skokova. Da bi se odredila verovatnoća nedetekcije za dati sinhroprefiks, pretpostavlja se da kanal ostaje u istom stanju tokom kratkog prefiksa. Analizirajući ovu aproksimaciju može se zapaziti da će ona dati optimistički rezultat za verovatnoću nedetekcije kada je kanal u dobrom stanju na početku sinhroprefiksa, zato što bi prelazak kanala u loše stanje povećao ovu verovatnoću. S druge strane, ako je kanal bio u lošem stanju na početku sinhroprefiksa, ova aproksimacija će dati pesimistički rezultat, budući da bi prelazak kanala u dobro stanje znatno smanjio verovatnoću nedetekcije. Imajući u vidu prethodna razmatranja, može se zaključiti da ova pretpostavka vodi do grešaka aproksimacije koje imaju tendenciju da se kompenzuju. Koja tendencija je veća zavisi od konkretnog izbora parametara.

Analiza performansi

Pretpostavlja se da su na ulazu prijemnika prisutni dolazeći korisni signal, aditivni beli Gausov šum i nekoliko širokopojasnih smetnji, koje mogu biti posledica ometanja. Na osnovu centralne granične teoreme, zbir belog Gausovog šuma i nekoliko širo-

kopojasnih smetnji takođe ima Gausovu raspodelu amplituda, pa se može tretirati kao beli Gausov šum. Neka je sa η označena efektivna jednostrana spektralna gustina snage ovog šuma na ulazu prijemnika.

Analiza performansi modifikovane kodne sinhronizacije sa tri nivoa izvršena je za slučaj kada pasivni korelator ima strukturu prikazanu na slici 4, a aktivni korelator strukturu prikazanu na slici 5. Pretpostavlja se da je trajanje čipa preambule jednako trajanju čipa dugog PS koda, tj. $T_p = T_c = T_h$.

Neka je sa f_0 označena centralna učestanost filtera propusnika opsega sa limiterom i neka su F_i učestanosti nosioca, pri čemu je $F_i = f_i + f_0$. Kada se pojavi odgovarajući sinhroprefiks, koji predstavlja povorka signala od m učestanosti ($F_m, F_{m-1}, F_{m-2}, \dots, F_3, F_2, F_1$), signal na izlazu sabirača sa slike 4 je suma kvadrata od m Rajsovih promenljivih. Verovatnoća da sinhroprefiks nije detektovan na pasivnom korelatoru, iako u stvarnosti on postoji, odgovara verovatnoći da napon na izlazu iz sabirača nije premašio prag t_{pc} . Ova verovatnoća može biti izražena u obliku komplementa generalizovane Marcumove Q-funkcije. Označimo generalizovanu Marcumovu Q-funkciju sa $Q_M(a, b)$, a njen komplement $(1 - Q_M(a, b))$ sa $Q_c^M(a, b)$, gde je

$$Q_M(a, b) = \int_b^\infty \xi (\xi/a)^{M-1} \exp \left[-\frac{(a^2 + \xi^2)}{2} \right] I_{M-1}(a\xi) d\xi \quad (15)$$

$X=1, 2, \dots \quad a, b \geq 0$

Generalizovana Q_M funkcija može se aproksimativno izračunati na sledeći način [10]:

$$Q_M(a, b) = \text{erfc}(y) \quad (16)$$

$$\text{gde je } y = (b^2 - a^2 - 2M)/(2\sqrt{a^2 + M}) \quad (17)$$

Argument b je normalizovani prag t_{pc} pasivnog korelatora. Njegova vrednost iznosi $(2t_{pc}^2\eta/T_h)$. Startni signal du-

gog PS koda generiše se u svakom trenutku odlučivanja u kojem je premašen prag.

Neka je $P_{fdl}(i/G)$ verovatnoća nedetekcije sinhroprefiksa na i -tom pasivnom korelatoru kada ne postoji feding u kanalu i neka je $P_{fdl}(i/B)$ verovatnoća nedetekcije sinhroprefiksa na i -tom pasivnom korelatoru kada postoji feding u kanalu. Korišćenjem izraza za verovatnoće stanja kanala tokom i -tog sinhroprefiksa $P_G(i)$ i $P_B(i)$, verovatnoća nedetekcije i -tog sinhroprefiksa na i -tom pasivnom korelatoru je:

$$P_{fdl}(i) = P_G(i)P_{fdl}(i/G) + P_B(i)P_{fdl}(i/B) \quad (18)$$

Neka je sa E_h označena primljena energija signala po skoku preambule u dobrom stanju kanala, a sa E'_h primljena energija signala po skoku preambule u lošem stanju kanala.

Ako se stanje kanala menja polako, tako da kanal ostaje u istom stanju tokom trajanja svih m skokova kratkog sinhroprefiksa, verovatnoće uslovne nedetekcije i -tog pasivnog korelatora, kada u kanalu nije i kada u kanalu jeste prisutan feding, $P_{fdl}(i/G)$ i $P_{fdl}(i/B)$, respektivno su:

$$P_{fdl}(i/G) = Q^c_m \left(\sqrt{2m \frac{E_h}{\eta}}, t_{pc} \right) \quad (19)$$

Sl. 4 — Struktura pasivnog korelatora

Sl. 5 — Struktura aktivnog korelatora

$$P_{fal}(i/B) = Q^c_m \left(\sqrt{2m \frac{E'_h}{\eta}}, t_{pc} \right) \quad (20)$$

Verovatnoća lažnog alarma na i-tom pasivnom korelatoru, $P_{fal}(i)$, koja označava da je prag t_{pc} premašen kada i-ti sinhroprefiks nije prisutan, može se opisati na sledeći način:

$$P_{fal}(i) = Q_m(O, t_{pc}) \quad (21)$$

Da bi se povećala pouzdanost odluke, u aktivnom korelatoru vrši se korelacija nad k skokova, pri čemu je $k \gg m$. Realno je pretpostaviti da je interval aktivnog korelatora k duži od srednjeg trajanja fedinga D . Zbog toga, deo od k skokova dugog PS koda koji je pod fedingom jednak je verovatnoći fedinga F .

Ukoliko je generisan (ispravno ili pogrešno) startni signal dugog PS koda, startuje se aktivni korelator. Verovatnoća lažnog alarma na izlazu aktivnog korelatora može se opisati relacijom:

$$P_{fa2} = Q_k(O, t_{ac}) \quad (22)$$

gde je sa t_{ac} označen prag sa kojim se izlaz aktivnog korelatora upoređuje.

Verovatnoća da aktivni korelator, koji je ispravno startovan, ne detektuje prisutno sinhrostanje, tj. napon na izlazu aktivnog korelatora ne premaši napon praga ($2t_{ac}^2\eta/T_h$), iznosi:

$$P_{fd2} = Q^c_k \left(\sqrt{2k \left[(1-F) \frac{E_h}{\eta} + F \frac{E'_h}{\eta} \right]}, t_{ac} \right) \quad (23)$$

Izračunavanje verovatnoće greške pri prenosu poruke o početnom stanju DPSK generatora zavisi od tipa primenjene modulacije — demodulacije. U opštem slučaju važi sledeća relacija:

$$P_e = (1-F)(P_e)_G + F(P_e)_B \quad (24)$$

gde $(P_e)_G$ i $(P_e)_B$ označavaju verovatnoće greške po bitu u dobrom i lo-

šem stanju kanala, respektivno. S obzirom na to da je $(P_e)_G \leq 10^{-2}$ i $(P_e)_B = 1/2$, verovatnoća greške pri prenosu poruke o početnom stanju DPSK generatora približno se može opisati relacijom:

$$P_e \cong \frac{F}{2} \quad (25)$$

U slučaju kada je $F=0,1$ verovatnoća greške je $P_e \cong 5 \cdot 10^{-2}$. Ova vrednost je neprihvatljivo visoka, pa se mora primeniti neki tip zaštitnog kodovanja.

Najjednostavniji tip zaštitnih kodova koji dozvoljava različite iznose redundanse je repetitivni kod. Korišćenje repetitivnog koda kod brzih ili sporih FS sistema sa učešljavanjem bita često je veoma efikasan metod za smanjivanje verovatnoće greške. Kod ovog koda, jedan informacioni bit je kodovan blokom od n_2 identičnih bita, pri čemu je n_2 neparan broj. Ovakav kod označava se sa $(n_2, 1)$ i sadrži samo dve kodne reči: »sve nule« i »sve jedinice«.

S obzirom na to da repetitivni kod $(n_2, 1)$ može da izvrši korekciju najviše $(n_2-1)/2$ grešaka, verovatnoća ispravnog dekodovanja primljene kodne reči na binarnom simetričnom kanalu je [17]:

$$P_b = \sum_{i=0}^{\frac{(n_2-1)}{2}} \binom{n_2}{i} P_e^i (1-P_e)^{n_2-i} \quad (26)$$

Verovatnoća P_b može postati proizvoljno bliska jedinici ukoliko je kodna reč dovoljno duga. S obzirom na to da se poruka o početnom stanju generatora dugog PS koda sastoji od reda deset bita, dužina kodne reči repetitivnog koda nije ograničavajući faktor.

Na osnovu relacija (2), (5) i (19) do (23) mogu se izračunati verovatnoća lažnog hvatanja P_{fl} i verovatnoća nedetekcije P_{miss} . Najteži zadatak pri projektovanju bloka za kodnu sinhronizaciju je da se na odgovarajući način odrede pragovi t_{pc} i t_{ac} .

Vreme uspostavljanja sinhronizacije

Kod tronivoske kodne sinhronizacije, neposredno pre početka emitovanja podataka, predajnik šalje uvodnik poruke. Dužina uvodnika predstavlja maksimalno vreme koje prijemnik ima na raspolaganju za uspostavljanje kodne sinhronizacije. Ovo vreme mora biti dovoljno dugo potencijalnom prijemniku da uspostavi sinhronizaciju sa velikom verovatnoćom.

Prema tome, vreme uspostavljanja sinhronizacije može se opisati sledećom relacijom:

$$T_A = (L + N_2 n_2 + k) T_h \quad (27)$$

Za $L=320$, $N_2=11$, $n_2=17$, $k=512$ i brzinu skakanja od 2000hop/s, vreme uspostavljanja sinhronizacije je $T_A \cong 0,51s$.

Numerički rezultati

Numerička izračunavanja u ovom radu su vršena uglavnom za slučaj da je kanal u stanju fedinga 15% vremena, tj. $F=0,15$. Na osnovu relacije (25) dobija se da je verovatnoća greške u tom slučaju $P_e \cong 7,5 \cdot 10^{-2}$. Ukoliko je primenjen repetitivni kod (17,1), na osnovu relacije (26), dobija se da je verovatnoća ispravnog dekodovanja primljene kodne reči $P_b \cong 0,99999895$. Ukoliko se poruka o početnom stanju DPSK generatora sastoji od $N_2=11$ bita, verovatnoća da je ova poruka ispravno prenet, na osnovu relacije (2), je $P_m \cong 0,9999885$.

Pod pretpostavkom da je srednje trajanje fedinga 64 skoka ($D=64$) i da je nominalna brzina skakanja 2000hop/s, trajanju fedinga odgovara vreme od $\tau_F=32ms$. Ovo su tipične vrednosti koje odgovaraju KT kanalu. Imajući u vidu relacije (10) i (11), verovatnoće prelaza za ovaj primer su $P_{bg} \cong 0,015625$ i $P_{gh} \cong 0,0027573$.

Verovatnoća da kanal ostaje u dobrom stanju unutar kratkog intervala

trajanja sinhro prefiksa od 16 skokova ($m=16$), ako je bio u dobrom stanju na početku intervala, iznosi $(1 - P_{gh})^{16} \cong 0,957$. S druge strane, ako je kanal bio u lošem stanju na početku sinhro prefiksa, verovatnoća da će kanal ostati u istom stanju za vreme trajanja sinhroprefiksa je $(1 - P_{bg})^{16} \cong 0,777$. Ova aproksimacija dovodi do grešaka koje su relativno male i, što je posebno važno, imaju tendenciju da se kompenzuju. Proračuni za druge vrednosti trajanja fedinga i brzine skakanja do vode do istih zaključaka.

Problem optimizacije podrazumeva minimizaciju verovatnoće nedetekcije P_{miss} pod uslovom da je verovatnoća lažne sinhronizacije P_{fl} manja od neke specificirane vrednosti. To se postiže odgovarajućim postavljanjem pragova t_{pc} i t_{ac} . Optimalan par pragova (t_{pc}, t_{ac}) daje minimum verovatnoće nedetekcije P_{miss} .

Sl. 6 — Verovatnoća lažnog hvatanja u funkciji pragova

($F = 0,15$; $df = 25 dB$; $D = 64$; $m = 16$; $L = 320$; $N_{pc} = 4$; $N_2 = 11$; $k = 512$; $N_{ac} = 1$)

Na slici 6 prikazana je verovatnoća nedetekcije u funkciji pragova t_{pc} i t_{ac} . Ravna površina predstavlja skup tačaka koje zadovoljavaju uslov $P_{fl} \leq 10^{-8}$. Svaka tačka je određena parom pragova (t_{pc}, t_{ac}) . Može se uočiti da beskonačno mnogo parova pragova (t_{pc}, t_{ac}) zadovoljava ovaj uslov. Optimalan

par pragova je onaj par (t_{pc}, t_{ac}) koji daje minimum verovatnoće nedetekcije:

$$P_M = \min\{P_{miss}\} \tag{28}$$

U tabeli 1 prikazane su vrednosti karakteristika fedinga i parametara sinhronizacije koje se koriste za numerička izračunavanja. Prikazane vrednosti karakteristika fedinga su tipične za ovaj tip kanala i one se najčešće koriste u literaturi [8]. Vrednosti parametara sinhronizacije odgovaraju realnom radio uređaju srednje složenosti.

Svi dijagrami su prikazani u opsegu E_b/η između 1 i 8 dB. U slučaju sistema sa brzim FS, gde se jedan bit prenosi u tri skoka, opseg E_b/η od 1 do 8 dB odgovara opsegu E_s/η između 6 i 13 dB. Ovaj opseg vrednosti je od interesa za prenos poruka u radio-komunikacijama.

U referenci [18] detaljno je analiziran uticaj svih karakteristika fedinga i parametara sinhronizacije na performanse kodne sinhronizacije. S obzirom da na složenost, a samim tim i na cenu, predloženog rešenja kodne sinhronizacije najviše utiče broj pasivnih i aktivnih korelatora, u ovom radu su analizirana samo ova dva parametra sinhronizacije.

Minimum verovatnoće nedetekcije računat je za najgori slučaj, tj. pod uslovom da je početak preambule (prvi sinhroprefiks) pod fedingom.

Uticaj broja pasivnih korelatora

Na slici 7 je prikazan minimum verovatnoće nedetekcije u funkciji broja pasivnih korelatora, pri čemu je odnos E_b/η važeći parametar. Povećava-

Sl. 7 — Minimum verovatnoće nedetekcije u funkciji broja pasivnih korelatora, odnos E_b/η je parametar
($P_{fl} \leq 10^{-8}$; $F = 0,15$; $df = 25$ dB; $D = 64$; $m = 16$; $L = 320$; $N_2 = 11$; $k = 512$; $N_{ac} = 1$)

Tabela 1

Primer karakteristika fedinga i parametara sinhronizacije

Oznaka	Parametar	Vrednost
F	Verovatnoća fedinga	0,15
df	Dubina fedinga	25 dB
D	Srednje trajanje fedinga	64 skokova
m	Dužina sinhro prefiksa	16 skokova
L	Dužina preambule	320 skokova
N_{pc}	Broj pasivnih korelatora	4
N_2	Dužina poruke o poč. stanju	11 bita
k	Dužina aktivnog korelatora	1024 skokova
N_{ac}	Broj aktivnih korelatora	1

njem broja pasivnih korelatora N_{pc} , verovatnoća nedetekcije se može značajno smanjiti. Ukoliko je $E_h/\eta \leq 1$ dB, minimum verovatnoće nedetekcije linearno opada sa porastom broja pasivnih korelatora. Ukoliko je $E_h/\eta \geq 3$ dB, minimum verovatnoće nedetekcije se može smanjiti za tri reda veličine (sa $3 \cdot 10^{-2}$ na $3 \cdot 10^{-4}$) sa povećanjem broja pasivnih korelatora sa dva na šest. Povećanje broja pasivnih korelatora iznad osam ne dovodi do smanjenja minimuma verovatnoće nedetekcije. Prema tome, možemo smatrati da je $N_{pc} = 8$ optimalan izbor ukoliko cena nije ograničavajući faktor.

Uticaj broja aktivnih korelatora

Na slici 8 prikazan je minimum verovatnoće nedetekcije u funkciji broja aktivnih korelatora pri čemu je odnos E_h/η važeći parametar. Povećanje broja aktivnih korelatora je efikasan na-

Sl. 8 — Minimum verovatnoće nedetekcije u funkciji broja aktivnih korelatora, odnos E_h/η je parametar
($P_{fl} \leq 10^{-8}$; $F = 0,15$; $df = 25$ dB; $D = 64$; $m = 16$; $L = 320$; $N_{pc} = 4$; $N_2 = 11$; $k = 512$)

čin za smanjenje verovatnoće blokiranja pri malim vrednostima odnosa E_h/η . Ukoliko je $E_h/\eta \leq 1$ dB, povećanje broja aktivnih korelatora dovodi do smanjenja verovatnoće blokiranja, a samim tim i do smanjenja P_M . Pri tom

treba naglasiti da povećanje broja aktivnih korelatora iznad tri nema opravdanja jer dovodi do veoma malog smanjenja minimuma verovatnoće nedetekcije. Ukoliko je $E_h/\eta \geq 3$ dB, povećanje broja aktivnih korelatora ne utiče na P_M . Prema tome, ukoliko se projektuje jeftin i relativno jednostavan uređaj, $N_{ac} = 1$ predstavlja optimalan izbor. Ukoliko se radi o složenom i skupom sistemu, preporučuje se $N_{ac} = 3$ kao kompromis između cene i kvaliteta.

Zaključak

U ovom radu prikazan je i analiziran novi metod protivelektronske zaštite, modifikovano uspostavljanje kodne sinhronizacije signala na tri nivoa sa frekvencijskim skakanjem, koji je pogodan za primenu u prisustvu fedinga. Metod ove sinhronizacije koristi skup pasivnih korelatora, demodulator poruke i banku aktivnih korelatora. Pasivni korelatori su podešeni na kratke sinhroprefikse (kratke PS kodove), kojima je modulisan nosilac. Primena više sinhroprefiksa smanjuje verovatnoću nedetekcije signala u uslovima fedinga. Kada je nadmašen nivo praga na izlazu bilo kog pasivnog korelatora, aktivira se demodulator koji »čeka« da primi poruku o početnom stanju generatora dugog PS koda. Nakon detekcije ove poruke, aktivira se jedan od aktivnih korelatora iz banke. Aktivna korelacija dugog PS koda obavlja se unutar dužeg vremenskog intervala, čime je obezbeđena visoka pouzdanost odluke. Ovaj metod obezbeđuje da generator dugog PS koda startuje iz drugog početnog položaja, svaki put kada se sistem koristi za komunikaciju.

Izvršena analiza i dobijeni rezultati pokazuju da je optimizacija parametara kodne sinhronizacije na tri nivoa u prisustvu šuma, smetnji i fedinga složen zadatak. Verovatnoća nedetekcije, kao kriterijum za ocenu uspešnosti kodne sinhronizacije, zavisi od brojnih karakteristika fedinga i para-

metara sinhronizacije. Zbog toga nije moguće izvući jednostavan zaključak. U zavisnosti od predviđene cene uređaja, moguće je, na različite načine, optimizovati sistem. S obzirom na to da su uređaji koji se projektuju za rad u kanalima sa fadingom, po pravilu, relativno složeni i skupi, preporučuje se korišćenje skupa od osam pasivnih korelatora za detekciju preambule i banke od tri aktivna korelatora za verifikaciju uspostavljene kodne sinhronizacije. Minimum verovatnoće nedetekcije koji se postiže za ove vrednosti parametara prikazan je na slici 9. Može se uočiti da ovakav izbor parametara obezbeđuje minimum verovatnoće nedetekcije $P_M < 10^{-3}$ za $E_h/\eta \geq 1\text{dB}$, a $P_M < 3 \cdot 10^{-5}$ za $E_h/\eta \geq 3\text{dB}$.

Sl. 9 — Minimum verovatnoće nedetekcije u funkciji odnosa E_h/η ,

($P_{fl} \leq 10^{-8}$; $F = 0,15$; $df = 25\text{ dB}$; $D = 64$; $m = 16$; $L = 320$; $N_{pc} = 8$; $N_z = 11$; $k = 512$; $N_{ac} = 3$)

Literatura:

- [1] Pickholtz, R. L. et al.: The Theory of Spread Spectrum Communications — A Tutorial, IEEE Trans. on Commun., Vol. COM-30, No. 5, May 1982, pp. 855—884.
- [2] Sage, G. F.: Serial Synchronization of Pseudonoise Signals, IEEE Trans. Commun. Techn., Vol. COM-12, No. 12, December 1964, pp. 123—127.
- [3] Hopkins, P. M.: A Unified Analysis of Pseudonoise Synchronization by Envelope Correlation, IEEE Trans. on Commun., Vol. COM-25, No. 8, August 1977, pp. 770—778.
- [4] Polydoros, A., and Veber, C.L.: A Unified Approach to Serial Search Spread Spectrum Code Acquisition, Parts I and II, IEEE Trans. on Commun., Vol. COM-32, No. 5, May 1984, pp. 542—560.
- [5] Jovanović, V. M.: Analysis of Strategies for Spread Spectrum Code Acquisition — Direct Approach, IEEE Trans. on Commun., Vol. COM-36, No. 12, December 1988, pp. 1208—1220.
- [6] Glišić, S. G.: A Novel Frequency Hopping Spread Spectrum Receiver Synchronization Scheme, Proc. of IEEE Global Comm. Conf. (GLOBECOM '84), Atlanta (Georgia, USA), November 26—29, 1984, paper, 29.2.
- [7] Rappaport, S. S. and Schilling, D. L.: A Two-Level Coarse Code Acquisition Scheme for Spread Spectrum Radio, IEEE Trans. on Comm., Vol. COM-28, No. 9, September 1980, pp. 1734—1742.
- [8] Wilson, N. D. et al.: Rapid Acquisition Scheme for Spread Spectrum Radio in a Fading Environment IEE Proc., Vol. 135, Pt. F, No. 1, February 1988, pp. 95—103.
- [9] Glišić, S. G., and Pajković, M. Đ.: Transient Response of Two-Level Coarse Code Acquisition in Spread Spectrum Radio, Proc. of Military Comm. Conf. (MILCOM '89), paper 49.5.
- [10] Rappaport, S. S.: Computing Approximations for the Generalized Q Function and Its Complement, IEEE Trans. on Information Theory, Vol. IT-17, July 1971, pp. 497—498.
- [11] Todorović, B., Delević, M.: A Method of Multilevel Code Synchronization for Spread Spectrum Radio Communications, Proc. of 32nd Symposium ETAN in Marine, Zadar (Yugoslavia), 1990.
- [12] Glišić, S., Todorović, B., Popović-Lavrinšek, M.: A New Approach to Long Code Acquisition in Spread Spectrum Radio, Proc. of IEEE Military Comm. Conf. (MILCOM 91), Mc Lean (Virginia, USA), December 1991, paper 56.2.
- [13] Šunjevarić, M., Todorović, B.: Mobilne radio-komunikacije, Komunikativna naučnotehnička informacija, VTI, Beograd, 1995.
- [14] Gilbert, E. N.: Capacity of a Burst-Noise Channel, The Bell System Technical Journal, September 1960, pp. 1253—1265.
- [15] Kanal, L. N., Sastry, A. R. K.: Models for Channels with Memory and Their Applications to Error Control, Proc. of the IEEE, Vol. 66, No. 7, July 1978, pp. 724—744.
- [16] Jennings, A.: Matrix Computation for Engineers and Scientists, John Wiley and Sons, New York, 1978.
- [17] Michelson, A. M., Levesque, A. H.: Error-Control Techniques for Digital Communication, John Wiley and Sons, New York, 1985.
- [18] Todorović, B.: Novi metod uspostavljanja kodne sinhronizacije radio-uređaja sa frekvencijskim skakanjem u kanalima sa fadingom, Doktorska disertacija, u pripremi.
- [19] Trivunčić, D.: Diplomatski rad, VTF, Beograd, 1993.
- [20] Raspopović, D.: Diplomatski rad, VTF, Beograd, 1993.
- [21] Lepir, D.: Seminarski rad, ETF, Beograd, 1994.