

სკრემბლირების უმარტივესი ალგორითმი სიგნალის სიხშირული გარდაქმნის დროს

მარინა ქურდაძე¹, მამუკა გოგაძე²

¹პროფესორი, საქართველოს ტექნიკური უნივერსიტეტი, ციფრული სატელეკომუნიკაციო ტექნოლოგიების აკადემიური დეპარტამენტის უფროსი. 555441020, m.kurdadze@gtu.ge, orcid- 0009-0001-2918-3328

²დოქტორანტი, საქართველოს ტექნიკური უნივერსიტეტი, ციფრული სატელეკომუნიკაციო ტექნოლოგიების აკადემიური დეპარტამენტი. 555742525 mamukagogadze01@gmail.com

რეზიუმე

მოცემული ნაშრომი იკვლევს სიგნალის ამპლიტუდის, სიხშირისა და დროის პარამეტრების გამოყენებით სკრემბლირების ალგორითმების ვარიანტებს. კვლევის მთავარი მიზანია დაადგინოს, რომელი პარამეტრი – სიხშირული, ამპლიტუდური თუ დროითი – გამოიყენება ყველაზე ხშირად სკრემბლირებაში, მათი სხვადასხვა პარამეტრებისა და კომბინაციების გათვალისწინებით.

განსაკუთრებული ყურადღება ეთმობა რადიოკავშირის სისტემებს, სადაც რადიოარხში არსებული ხელშეშლები მნიშვნელოვნად ართულებს სამეტყველო სიგნალის ამპლიტუდის ზუსტ აღდგენას. ამ კონტექსტში, ნაშრომი დეტალურად განიხილავს ამპლიტუდური გარდაქმნის ალგორითმს სკრემბლირებაში. მიუხედავად იმისა, რომ ეს ალგორითმი პრაქტიკულად არ გამოიყენება ზოგიერთ შემთხვევაში, იგი გათვალისწინებულია საინტერესო მიდგომებს შემდგომი კვლევებისთვის, განსაკუთრებით ციფრულ ფორმატში სკრემბლირების კოდირების კუთხით.

ნაშრომში ასევე წარმოდგენილია და დასაბუთებულია სიგნალის სიხშირული გარდაქმნის ალგორითმი და შესაბამისი მიდგომები სკრემბლირების სხვადასხვა სახეობებისთვის.

საკვანძო სიტყვები: სკრემბლირება, ალგორითმი, ამპლიტუდა, სიხშირე, კრიპტოალგორითმები, არასანქცირებული, ამპლიტუდური.

შესავალი

საკომუნიკაციო კავშირის სისტემით სარგებლობის აუცილებელი და უპირველესი პირობაა გარეშე პირთა წვდომისაგან ინფორმაციის დაცვა. ინფორმაცია საიმედოდ არის დაცული ციფრული სტანდარტის ფიქურ სისტემებში, სადაც გამოიყენება კრიპტოგრაფიული მეთოდები - კრიპტოალგორითმები, რომლითაც უზრუნველყოფილია დაცვის მაღალი ხარისხი არასანქცირებული წვდომისაგან. ნაშრომში გაანალიზებულია სასურველი შედეგის

მიღებამდე, სკრემბლირების ყველა შესაძლო შესასრულებელი ვარიანტები, კერძოდ: სიგნალის სპექტრის გარდაქმნის ალგორითმი; სალაპარაკო სიგნალის სიხშირის ზოლის დაყოფის ალგორითმი (რამდენიმე ქვედიაპაზონის საშუალო სიხშირე); სალაპარაკო სიგნალის სიხშირედ ზოლის რამდენიმე ქვედიაპაზონად დაყოფის ალგორითმი და მათი სიხშირული გადაწყობის ალგორითმის სინთეზი. [3]

ძირითადი ნაწილი

ციფრულ რადიოსადგურზე დაფუძნებული ტელეკომუნიკაციის მიმართულება-მობილური კავშირი, შესამჩნევად უპირატესია ანალოგიურთან შედარებით, სადაც ინფორმაციის კონფიდენციალურობის სურვილი არ იკლებს. ზოგჯერ საჭიროა ინფორმაციის გარანტირებული დაცვა და საკმარისი გახდეს გადასაცემი ინფორმაციის გაურჩევლობა, რომლის ოპტიმალური გადაწყვეტაა სკრემბლერის გამოყენება [2].

ციფრული სიგნალის სკრემბლირება გულისხმობს საწყისი სალაპარაკო სიგნალის იმგვარად გარდაქმნას, რომ მას ჰქონდეს სალაპარაკო სიგნალისათვის დამახასიათებელი მინიმალური ნიშანი, რის შედეგადაც სიგნალი გახდება ამოუცნობი, გაურკვეველი. ამავდროულად იგი დაიკავებს იგივე სიხშირულ ზოლს, რაც ქონდა საწყის სიგნალს. ასეთი გარდაქმნის აუცილებელი თვისებაა მისი უკუგარდაქმნის შესაძლებლობა, რათა მოხერხდეს სიგნალის აღქმა მიმღებ მხარეს.

ტექნიკური საშუალებები, რომლებიც უზრუნველყოფენ ინფორმაციის ამ მეთოდით გარდაქმნას, ანუ სკრემბლერები, ცნობილია ინფორმაციის შემნიღბველები. როგორც წესი სკრემბლირების მეთოდით დაცულ სასაუბრო სიგნალებს მაინც აქვთ ხოლმე ღია, დაუცველი სასაუბრო სიგნალის სახე.

ზოგიერთ შემთხვევაში პრაქტიკულად, ინფორმაციის დაცვის ანალოგური ხერხები უფრო ადვილად გამოსაყენებელია, იაფია და აღდგენილი სიგნალიც უფრო მაღალი ხარისხისაა, მაგრამ ნაკლებ დაცულია ვიდრე ციფრულები,

სკრემბლირებით სიგნალის გარდაქმნა, რომელიც სამი პარამეტრითაა შესაძლებელი, (ამპლიტუდა, სიხშირე და დრო). რადიოკვშირის სისტემებში უფრო მეტად გამოიყენება სიხშირული და დროითი გარდაქმნა და მათი კომბინაცია. [6] საგულისხმოა, რომ ხელშემშლელი რადიოარხში საგრძნობლად ართულებს სალაპარაკო სიგნალის ამპლიტუდის ზუსტ და ამპლიტუდური გარდაქმნა სკრემბლირებაში პრაქტიკულად არ გამოიყენება.

მობილურ სისტემებში სიგნალის სიხშირული გარდაქმნის დროს გამოიყენებული სკრემბლირების სახეები: სიგნალის სიხშირული ინვერსია ანუ სიგნალის სპექტრის გარდაქმნა; სალაპარაკო სიგნალის სიხშირის ზოლის დაყოფა რამდენიმე ქვედიაპაზონად და მათი სპექტრის ინვერსია უშუალოდ თითოეულში ქვედიაპაზონის საშუალო სიხშირედ; სალაპარაკო სიგნალის სიხშირედ ზოლის დაყოფა რამდენიმე ქვედიაპაზონად და მათი სიხშირული გადაწყობა. შეიძლება დალაგდეს წინდაწინ შერჩეული ალგორითმით, რომელსაც კონკრეტული სიგნალისთვის ინდივიდუალურად ვარჩევთ და თემატურ სახეს ვაძლევთ მსგავსი სიგნალების შემთხვევაში [4]. საგულისხმოა ამ ალგორითმებთან ერთად დროითი გარდაქმნის ალგორითმების შერჩევაც და მათი კომპლექსური გამოყენება რომლის დროსაც უფრო გამარტივებული იქნება სიგნალის დაშლა სალაპარაკო სეგმენტებად და მათი დროში

გადაწყობის საუბრის სეგმენტების ინვერსიის ალგორითმით და სასაუბრო სეგმენტების დროითი გადაწყობის ალგორითმით.

ეს მიგნება გვთავაზობს ერთდროულად იქნას გამოყენებული, როგორც სიხშირული ასევე დროითი სკრემბლირების რამოდენიმე ალგორითმი, შერჩეული მისადაგებული ვარიანტებიდან.

სკრემბლირების ძირითად პარამეტრებთან ერთად მნიშვნელოვანია წყარო-მიმღებზე შედგენილი ალგორითმების სიზუსტის დაცვა, რომელიც სიგნალის უკუგარდაქმნისთვისაა და გულისხმობს სიგნალის გარდაქმნის კომბინირებულ მეთოდს ანუ სკრემბლერის გასაღებს, რომლის რაოდენობაც განისაზღვრება ყველა შესაძლო გასაღებების ვარიანტის სიმრავლით. ერთი (გასაღებს, ძირითადი) პარამეტრის მქონე სკრემბლერისათვის იგი განისაზღვრება ამ პარამეტრის შესაძლო მდგომარეობის რიცხვით, რამდენიმე პარამეტრიანი სკრემბლერისათვის - ამ პარამეტრების შესაძლო კომბინაციების რაოდენობით (როგორც წესი ყველა პარამეტრის მდგომარეობის წარმოებით).

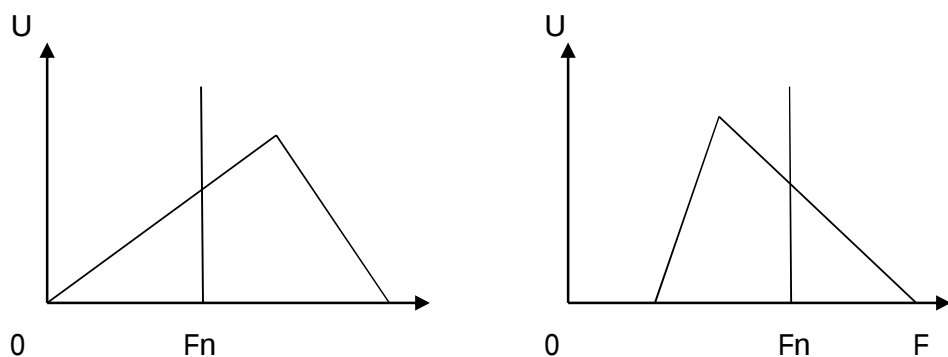
ცნობილია, რომ სიგნალის აღდგენის ხარისხი განისაზღვრება სიგნალის დამახინჯებით მისი სიხშირული და დროითი გარდაქმნისას. ფაქტობრივად ეს მახასიათებელი აისახება აღდგენილი საუბრის ხარისხით და ითვლება, რომ მსმენელი ძალისხმევით აღიქვამს საუბარს და შეტყობინების შინაარსს.

სიგნალის აღდგენის საუკეთესო ხარისხი აქვთ სიხშირულ ინვესტორებს, რომლებიც პრაქტიკულად არ აუარესებენ საუბრის გარჩევადობას სწორი რეალიზაციის დროს. სიხშირული გარდაქმნის შედარებით რთულმა მეთოდებმა შეიძლება გააჩინოს რაღაც დამახინჯებები სალაპარაკო სიგნალში. აღდგენილი საუბრის მაღალი ხარისხით აღდგენის რეალობას დროითი გარდაქმნის დროს, სჭირდება საკმაოდ რთული დამუშავება.

ნარჩენ გარჩევადობაში გულისხმობენ, ჩვეულებრივი მიმღებით, ან რადიოსადგურით (რომლებიც არ არიან შესაბამისი ანალოგური სკრემბლერით აღჭურვილი) მიღებული სკრემბლირებული სიგნალის აღდგენილი ფრაგმენტების გარჩევის პროცენტს.[4]

აღსანიშნავია ისიც, რომ ცნობილი ანალოგური სკრემბლერების უმრავლესობა რაღაც დონით მაინც ტოვებს ნარჩენ გარჩევადობას, სკრემბლირების მეთოდით დაცული საუბრის მოსმენისას რჩება გარკვეული ინფორმაცია საუბრის ტემბრზე, შესამჩნევია პაუზები საუბარში. შედარებით იოლი სახის სკრემბლირებით დაცულ სიგნალში გამოცდილ ოპერატორს შეუძლია სპეციალური მოწყობილობების გამოყენების გარეშე, ნარჩენი გაღრმავების ხარჯზე გამოიღოს გადაცემული საუბრის შინაარსი და აღადგინოს ინფორმაციის 10-50%, განსაკუთრებით მაშინ, როდესაც ცნობილია გადაცემული საუბრის თემა.

კვლევის შედეგად გამოიკვეთა, რომ გადაცემული ინფორმაციის სპექტრის სიხშირული ინვერსია სალაპარაკო სიგნალის ექვივალენტურია და სიგნალის სიხშირული ზოლის შემობრუნება ექვივალენტურია ნებისმიერი საშუალო (F_n) მიმართ. იხ. გარდაქმნის პრინციპი ნახაზ N 1-ზე.

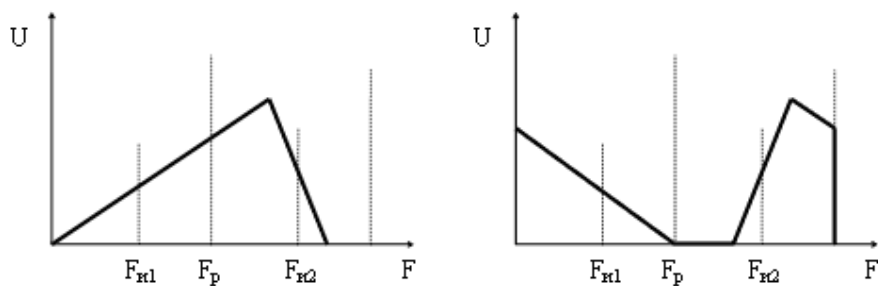


ნახ.1.

სიგნალის საწყისი სპექტრი და სიგნალი სპექტრული ინვერსია, იმ შემთხვევაში, როდესაც ვაძარებთ სიგნალის სიხშირულ ინვერსიას, გამოკვლეულია, რომ ამ პრიზმაში რთულ გარდაქმნას უზრუნველყოფს სკრემბლერი. მსგავს შემთხვევებში სიგნალის ზოლი იყოფა ქვედიაპაზონებად და ხორციელდება ამ ქვედიაპაზონების სიხშირული ინვერსია (ზოლის წამანაცვლებელი ინვერტორი). ამ დროს გამოიყენება და ცნობილია: -ზოლის დაყოფა ხდება ორ ქვედიაპაზონად და ასეთი გარდაქმნის პრინციპი ნაჩვენებია მე-2-ე ნახაზზე.

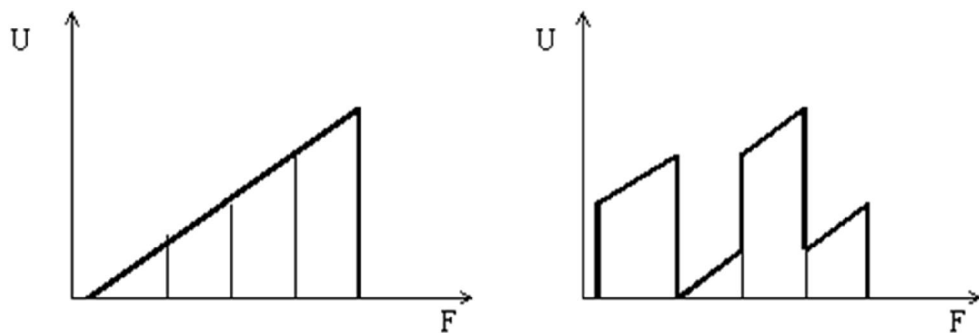
F_p - სიხშირე დაყოფილი სიგნალის სპექტრი

F_{o1} და F_{o2} - სიხშირის ინვერსია 1 და 2 ქვედიაპაზონად



ნახ.2.

ზოლური სკრემბლერები იყენებენ სალაპარაკო სიგნალის ზოლის რამდენიმე ქვედიაპაზონად დაყოფას და ამ დიაპაზონების სიხშირულ გადაწყობას. ასეთი ზოლური სკრემბლერის მუშაობის პრინციპი ნაჩვენებია მე-3-ე ნახაზზე, 4 ზოლის შემთხვევაში



ნახ. 3

ზოლური სკრემბლერი შეიძლება რეალიზებული იქნას ფურიეს სწრაფი გარდაქმნის პრინციპზე. ასეთი სკრემბლერის გადამცემ მხარეზე ხდება პირდაპირი ფურიეს სწრაფი გარდაქმნა, ზოლების სიხშირული გადაწყობა და შემდეგ უკუ ფურიეს სწრაფი გარდაქმნა. მიმღებ მხრეს განხორციელდება ანალოგური გარდაქმნა ზოლების სიხშირული უკუ გადაწყობით. ასეთი სახის სკრემბლერში შეიძლება მიიღწეს სიგნალის დაცვის მაღალი დონე, სიხშირული ზოლების გადაწყობის გაზრდის ხარჯზე, ოღონდაც სკრემბლირების ეს მეთოდი აქამდე იშვიათად გამოიყენება მობილური რადიოკავშირის სისტემებში რთული ტექნიკური მხარის გამო, მაგრამ ახლა უკვე მისი ეს დახვეწილი და აპრობირებული მეთოდი, რომელიც ეფუძნება ფურიეს მწკრივის მიხედვით სწრაფ გარდაქმნას, კავშირის არხში შემოაქვს დროითი დაყოვნება და სკრემბლერი, როგორც მექანიზმი დადებითად მუშაობს მთელი სისტემის გამართულობაზე.

დასკვნა

სიგნალის გარდაქმნის ვარიანტების ცალ-ცალკე განხილვითა და დასმული ამოცანის გადაწყვეტის გზების სიმულაციით, მივიღეთ სკრემბლირების გამოკვეთილად სასურველი და უმარტივესი ალგორითმი. კვლევამ აჩვენა რომ გამოყენებული სიხშირული, ამპლიტუდური თუ დროითი პარამეტრი თავისი ბუნებით თუ კომბინაციით, ჩანაცვლებად რეჟიმში გადასვლის შემთხვევაში, თვითონ იმუშავებს განსაზღვრულობას და აქვს მკვეთრად გამოხატული სტრუქტურული მიდგომა რადიოარხში შესაძლო ხელშეშლების მიმართ, რომელიც საგრძნობლად ართულებდა სალაპარაკო სიგნალის ამპლიტუდის ზუსტ აღდგენას. ამასთან დაკავშირებით ნაშრომში დაზუსტდა სკრემბლირებაში ამპლიტუდური გარდაქმნის ალგორითმი. რომელსაც საკმაოდ საგულისხმო ანალიზი აქვს შემდგომი კვლევისთვის ციფრულ ფორმატში სკრემბლირების კოდირებისათვის. მიდგომების გაანალიზებით დასაბუთდა სიგნალის სიხშირული გარდაქმნის ალგორითმის უპირატესობა სკრემბლირების სახეების მიხედვით.

ლიტერატურა:

1. Anastasi G., Passarella A. (2023). Towards a Novel Transport Protocol for Ad hoc Networks. Proc. PWC 2023. Internet resource: <http://info.iet.unipi.it/~anastasi/papers/iscc05.pdf>
2. Harris Corporation, HF Technology. (2021). Edition 2, October. Radio Communications Inthe Digital Age. Internet resource: https://code7700.com/pdfs/radio_communications_in_the_digital_age.pdf
3. Leon W. Couch, William J. Weisz. Radio Spectrum Utilization. Internet resource: <https://www.sciencedirect.com/science/article/pii/B0122274105006402?via%3Dihub>
4. Army Techniques Publication *ATP 6-02.53. (2020). Techniques for Tactical Radio Operations. Internet resource: https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN20819