УДК 621.396.61/62 **DOI: 10.31673/2412-9070.2022.044244**

В. Л. ПАРХОМЕНКО, канд. техн. наук, ст. наук. співробітник;
А. С. ЩЕПАК, аспірант;
В. В. ПАРХОМЕНКО, ст. викладач;
А. І. БОНДАРЕНКО, аспірант,
Державний університет телекомунікацій, Київ

АВТОМАТИЧНИЙ ДОБІР ЧАСТОТ ПЕРЕДАВАННЯ ІЗ ЗАСТОСУВАННЯМ МЕТОДУ ФОРМУВАННЯ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ

У разі втрати зв'язку або для захисту каналу передавання в сучасних системах безпроводової пропагінації радіосигналу застосовують різноманітні методи. Одним із таких є зміна частот трансляції з використанням псевдовипадкових послідовностей. Він дає змогу завдяки нескладним розрахункам без надмірного перевантаження системи здійснювати планові чи позапланові зміни основної частоти передавання, які не можуть бути перехоплені чи виявлені звичайними методами. Отже, без зміни фізичних елементів системи можна досягти підвищення захищеності та стабільності пропагінації радіосигналу.

Один із можливих способів – послідовна заміна одночасно на приймачі та передавачі активної смуги передавання радіосигналу. Допускається також наявність додаткових резервних каналів. Важливим аспектом є синхронізація всіх складових частин системи для одномоментного переходу. Досягається вона наперед заданим алгоритмом, на основі якого формується псевдовипадкова послідовність, що збігається для кожного компонента системи. Результат обчислення алгоритму видає псевдовипадкові результати, що унеможливлює перехоплення або альтернативний розрахунок сторонніми спостерігачами за умови, що їм не відомі особливості роботи алгоритму.

Оскільки транслюється лише кодова послідовність, а доступ до алгоритму існує лише всередині системи, не є обов'язковим додаткове шифрування передавачем та подальше декодування приймачем отриманої послідовності, що позитивно впливає на швидкість роботи системи; обсяг інформації, що передається за одиницю часу; можливість ведення безперебійного передавання даних у режимі реального часу з мінімальною затримкою.

Ключові слова: формування псевдовипадкових послідовностей; фрактальні сигнали; кодований ключ.

Вступ

Практична важливість завдання побудови стійкого зв'язку за наявності великої кількості радіоелектронних завад останнім часом стрімко зросла. Спричинено це ситуаціями, коли можливість установлення стабільного проводового з'єднання відсутня, а трансляція ведеться в зовнішньому середовищі, насиченому значною кількістю сигналів від трансляторів, частота яких зумовлює їх вплив на передавання корисної інформації всередині системи.

На якість передавання сигналу можуть істотно впливати й інші сигнали подібної частоти або умови, коли обидва сигнали є похідною від сигналу однакової частоти. Також від частоти сигналу залежить чимало фізичних параметрів сигналу. А отже, зміна частоти іноді є обов'язковою умовою для підтримання стабільного з'єднання. Якщо приймач і передавач можуть підтримувати сигнали на кількох однакових діапазонах, то вони здатні змінювати діапазони передавання для підвищення якості зв'язку або забезпечення неперервного з'єднання.

Зміна частоти може відбуватись періодично, але для розв'язання непередбачуваних практичних проблем передавання, потрібна можливість зміни частоти навіть у разі раптового зникнення сигналу. Вочевидь, частоти приймача і передавача мають збігатись. За умови, що встановлення зв'язку після втрати комунікації повинні відбуватись якомога швидше, добирання частот навмання не дає змоги досягти задовільного результату. Отже, після втрати сигналу приймач та передавач мають миттєво перейти на нову частоту, яка не є визначеною заздалегідь, але буде однаковою для обох приладів. Задача досягнення такої умови розглядається в цій статті.

Основна частина

Важливою умовою працездатності системи є обмеження розміру передавання повідомлення для того, щоб відсоток корисної інформації під час трансляції істотно не зменшувався порівняно із заданими параметрами. Ця вимога дуже важлива, оскільки в разі вузького каналу передавання інформації можливість відправлення великих масивів даних зі значною вірогідністю буде відсутня. Алгоритм оброблення повідомлення також не має бути занадто ресурсозатратним, адже далеко не відомі системні характеристики пристрою оброблення. Проте для досягнення максимально можливої універсалізації варто припускати відсутність значних потужностей для оброблення заданого алгоритму.

Одним із варіантів розв'язання цієї задачі є обмін певним ключем, який би давав змогу одно-

значно вибрати частоту сигналу як для приймача, так і для передавача. Оскільки втрата сигналу буде помітна саме на приймачі, генерування ключа має відбуватися на боці передавача. Також у разі втрати сигналу та переходу на нову частоту приймання приймач має повідомити про це передавач, для цього або має існувати проміжок між циклами трансляції сигналу для приймання на частоті приймача, або приймач повинен здійснювати паралельне приймання на другій антені.

Одним із найактуальніших досліджень з цієї тематики є праця [1], в якій зазначається, що практичне використання псевдовипадкових сигналів у системах зв'язку викликає неабияку зацікавленість учених, конструкторів та інженерів і є одним із головних напрямів досліджень у галузі телекомунікацій та теорії передавання інформації. У статті [2] зауважено, що значна кількість праць, присвячених використанню шумоподібних сигналів в інфокомунікаційних системах, дає можливість дійти висновку щодо доцільності проведення досліджень методів синтезу нових сигналів, складних конструкцій, зокрема псевдохаотичних та фрактальних широкосмугових сигналів. Автори використовують відмінний від запропонованого спосіб генерування сигналів, проте наголошують на потребі в існуванні таких засобів шифрування інформації.

У цих та інших джерелах здійснено огляд сучасних проблем щодо передавання сигналу та способів їх подолання. Велику увагу приділено методу використання псевдовипадкових коливань. Практичні напрацювання в цій сфері використовуються в багатьох варіантах у сучасній радіоапаратурі, наприклад радіостанціях та інших засобах безпроводової комунікації.

Також у цих працях заслуговує на увагу саме шифрування та кодування сигналу, що безперечно є надзвичайно важливим. Пристрої, що працюють із використанням цих технологій шифрування, відповідають сучасним стандартам безпеки та вимогам до захищених технічних засобів зв'язку. Процес декодування сигналу стороннім агентом забирає занадто багато часу, тож шифроване повідомлення, навіть у разі перехоплення, можна вважати таким, до якого не має доступу жоден інший пристрій, що перебуває поза системою.

Утім, існують ситуації, коли немає потреби шифрувати повідомлення повністю, і генерування псевдовипадкового ключа слугує виключно для добирання потрібної в разі втрати зв'язку нової частоти. Це може бути зумовлено кількома факторами, наприклад: повідомлення вже закодовано; час розкодування повідомлення не дуже значний, але актуальність інформації в ньому втрачається значно швидше; обчислювальні потужності системи приймання/передавання не дають змоги здійснювати шифрування значних обсягів інформації без втрати часу, який є більш пріоритетним.

Прикладом такої системи може бути комплекс, основним завданням якого є неперервне передавання відеоінформації великого обсягу безпроводово в режимі реального часу. Застосування додаткового шифрування для такого сигналу потребує від процесора системи ресурсів, яких може не бути, через що трансляція перериватиметься або вестиметься із затримкою, яка не завжди є допустимою. Наприклад, якщо процес керування нестаціонарною системою залежить від даних, здобутих під час декодування переданої інформації.

Варто зауважити, що в процесі обчислення потрібно брати до уваги як час шифрування, так і час дешифрування, швидкість розбиття інформації на блоки та їх об'єднання. Доцільно вважати, що саме передавання сигналу здійснюється миттєво, оскільки таке передавання передбачається використовувати на незначних для швидкого поширення радіосигналу в середовищі відстанях. Надмірна затримка, що може виникнути внаслідок істотного збільшення часу обчислення через велику кількість процедур, пов'язаних із шифруванням, здатна зробити цей процес недоцільним.

Отже, метою цієї статті є розрахунок такого методу зміни частоти приймання/передавання сигналу, який би і задовольняв умови збереження швидкодії системи загалом, і давав змогу збільшити надійність та стресостійкість безпроводових систем передавання за наявності великої кількості радіоелектронних завад.

Аналіз задачі та її розв'язання розбито на два етапи. *Перший етап* — дослідження впливу на швидкість роботи системи таких факторів, як генерування коду для передавання; кодування додаткової інформації про резервні частоти трансляції; передавання збільшеного повідомлення; аналіз та збереження результатів до отримання повторної комунікації за можливості.

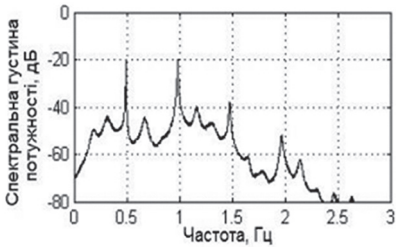
У такій системі генерування кожного наступного елемента псевдовипадкової послідовності досягається в такий спосіб:

$$x_n + 1 = x_n*(1 - x_n/K), \qquad (1)$$

де $x_n + 1$, x_n — актуальне та наступне значення, K — алгоритм, що видає псевдовипадковий результат обчислення.

Спектр результуючої потужності коливань, згенерований кільцевим автогенератором, і його залежність від частоти, що є результатом автоматичного генерування псевдовипадковим методом зображено на рисунку.

Цікавою особливістю кількох генераторів хаотичних коливань усередині замкненої системи є їх автоматична синхронізація після проходження всіх перехідних процесів. Це дає змогу дійти



Спектр потужностей псевдовипадкових коливань

висновку щодо можливості синхронізації всіх пристроїв усередині однієї системи безпроводового передавання інформації для стаціонарних і нестаціонарних пристроїв та їх комплектувальних.

Другий етап — обчислення позитивного впливу системи резервної зміни частот у разі раптової втрати встановленого з'єднання. Загалом це дасть можливість зробити висновок про прямий зв'язок між упровадженням завадозахищених методів комунікації в системі, збільшенням загальної стійкості та ресурсами, потрібними для виконання такої модернізації в уже наявних приладах.

Важливою вимогою до згенерованих випадковими методами послідовностей буде відповідність членів послідовності закону нормального розподілу, що б гарантувало максимальну захищеність передаваної інформації, особливо кодових послідовностей. Розраховується це так:

$$x_n + 1 = (a * x_n + b) mod m, \qquad (2)$$

де $x_n + 1$, x_n — члени послідовності; a, b, m — цілі числа, прості стосовно інших.

Висновки

Отже, завдяки застосуванню додаткових частот підвищується завадозахищеність системи; зростає вірогідність неперервного передавання повідомлень за умов впливу значної кількості радіоелектронних завад; зменшується ризик невідворотних збоїв, втрат зв'язку, інших негативних сценаріїв. Використання псевдовипадкових послідовностей дає змогу зберігати високий рівень захищеності під час передавання сигналу, не збільшуючи істотно час, потрібний на обчислення, передавання сигналу, що, зі свого боку, задовольняє обов'язкові умови для систем реального часу.

Для подальшого розвитку в цьому напрямі треба здійснювати покращення двома шляхами. Перший — застосуванням широкої смуги частот. Це дало б можливість збільшити варіативність частоти трансляції сигналу, що зрештою зменшило б вплив завад на дві сусідні вибрані частоти пропагінації через додаткове розходження на смугах. Такі методи можуть бути цікавим архітектурним вирішенням для багатьох застосувань, включно з компактними напрямленими антенами, радіолокаційними сигналами та радіомаяками, RFID-позначками далекого радіуса дії тощо [3]. Другий — постійною зміною частот. Для досягнення кращого результату в цьому разі потрібно, щоб передавання дублювалось одразу на кількох частотах, які не заважають одна одній, із поступовою зміною активних і резервних каналів.

Список використаної літератури

1. ***Політанський Р. Л.*** *Розроблення завадозахищенних систем передавання інформації на основі псевдовипадкових коливань та фрактальних сигналів: дис. на здобуття наук. ступеня докт. техн. наук. Львів, 2016. 142 с.*

2. ***Гресь О. В., Шпатар П. М., Політанський Р. Л.*** *Шифрування інформації з використанням псевдовипадкових гаусових послідовностей // II Міжнар. наук.-практ. конф. «Фізикотехнологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки» (м. Чернівці, жовтень, 2012 р.) Чернівці, 2012. С. 89.*

3. ***Circular*** *wire-bundle superscatterer / S. Kosulnikov, D. Vovchuk, R. Noskov [et al.] // Journal of Quantitative Spectroscopy and Radiative Transfer. 2022. URL:*

https://www.sciencedirect.com/science/article/abs/pii/S0022407322000024

V. L. Parkhomenko, A. S. Shchepak, V. V. Parkhomenko, A. I. Bondarenko

AUTOMATIC SELECTION OF TRANSMISSION FREQUENCIES USING THE METHOD OF FORMATION OF PSEUDO-RANDOM SEQUENCES

It is extremely important in many technological areas to provide stable wireless secure communication. A significant contribution to the final result is made by the shape of the transmitter antenna, and more precisely, the signal directional pattern of this antenna. For cases where a significant portion of the system requirements remain unknown, generally the best approach will be to follow universality. But, if the requirements for the final result are precisely defined, it is advisable to maximize efforts to achieve this or that final state. In this case, it will be more correct to choose the shape of the antenna depending on the final conditions, having previously weighed all the features of the available design solutions.

The article examines and compares two types of antennas — omnidirectional and narrowly directional. Their strengths and weaknesses are described; situations in which they can be applied and get better results compared to analogues at the same transmitter power. Selection of optimal parameters is carried out on the basis of predetermined information about the purpose and features of using the antenna on the transmitter. The considered information allows us to draw a conclusion about the advantage of narrowly directional antennas compared to omnidirectional ones in a situation where one of the main indicators is the distance between the transmitter and the receiver. Also, by changing such parameters as the angle width of a narrowly directional antenna, you can reduce the negative impact of the weaknesses of this type of transmitters. For example, a non-stationary object may accidentally leave the range of a stable radio signal from such an antenna, but the widening of the angle allows you to significantly reduce the probability of such a negative scenario.

Keywords: signal propagation; narrowly directed antennas; phased array.