При преобладании знаков 0 в числе r, например, со значением $\nu_0 = 0.75$, получаем выигрыш $\gamma = 1.573$. В пределе для числа $r = 2^m$ максимальный выигрыш достигает значения $\gamma_{max} = 1.82$. Это ясно, так как удвоение выполняется гораздо быстрее сложения точек. При преобладании единиц в последовательности r результат будет обратным. В частности, при $r = 2^m - 1$ минимальный выигрыш равен $\gamma_{min} = 1.193$. Заметим, что приведенные результаты относительно нижней границы γ в некоторой степени условны, так как мы приняли 1U = 0.5M. В частных случаях параметр d, использующийся при вычислении сложения точек, может принимать малые значения, тогда величиной 1U вообще можно пренебречь (при этом $\gamma_{min} = 1.249$).

В заключение резюмируем, что кривые Эдвардса имеют неоспоримые преимущества как перед каноническими эллиптическими кривыми, так и перед другими известными изоморфными формами кривых [5]. Главные из них – быстродействие и удобство программирования. Хотя класс этих кривых приблизительно в 4 раза уже класса всех кривых, их применение в криптосистемах перспективно.

Список литературы

1. Edwards H.M. A normal form for elliptic curves. Bulletin of the American Mathematical Society, Volume 44, Number 3, July 2007, Pages 393-422.

2. Bernstein Daniel J., Lange Tanja. Faster addition and doubling on elliptic curves. IST Programme under Contract IST–2002–507932 ECRYPT, 2007, PP. 1-20.

3. Bernstein Daniel J., Lange Tanja, Farashahi R.R. Binary Edwards Curves. IST Programme under Contract IST-2002-507932 ECRYPT, 2008, PP.1..23.

4. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых. Учеб. пособие. – К.: ІВЦ «Політехніка», 2004. – 224с.

5. Daniel J. Bernstein, Tanja Lange, Explicit-formulas database (2007). hyperelliptic.org/EFD.

Рецензент: Дудикевич В.Б.
Надійшла 9.06.2011

УДК 621.391

Кувшинов О.В., Жук О.Г., Бортнік Л.Л. Толюпа С.В.
(Військовий інститут телекомунікацій та інформатизації
Національного технічного університету України „
Київський політехнічний інститут", ДУІКТ)

НАПРЯМКИ ВДОСКОНАЛЕННЯ ТЕХНОЛОГІЇ OFDM ПРИ ВПЛИВІ НАВМИСНИХ ЗАВАД

В даний час технологія ортогонального частотного мультиплексування – OFDM (Orthogonal Frequency Division Multiplex) широко застосовується в мережах безпровідного доступу стандартів IEEE 802.11 та IEEE 802.16, системах цифрового радіомовлення T-DAB та DRM, цифрового телебачення DVB-T, xDSL-модемах тощо [1 – 5].

При формуванні OFDM-сигналу інформаційний потік зі швидкістю B ділиться на N паралельних підпотоків, швидкість кожного з яких в N разів менша (B/N). Кожний з цих підпотоків модулює індивідуальну піднесучу, які ортогональні між собою. Спектри сигналів на індивідуальних несучих перекриваються, але завдяки ортогональності сигнали розділяються на прийомі без спотворень. Група несучих частот, яка в даний момент часу переносить біти паралельних цифрових потоків, називається символом OFDM. Для модуляції піднесучих застосовують *КАМ-М* (*М*-позиційну квадратурну амплітудну модуляцію) або *ФМ-М* (*М*-позиційну фазову модуляцію) [2].

Переваги модуляції OFDM проявляються при великій (сотні і тисячі) кількості несучих *N*. Так, в стандарті IEEE 802.11*a* та IEEE 802.11*g* використовуються 52 несучих, в стандарті IEEE 802.16 – від 200 до 2048, в специфікації наземного цифрового телевізійного мовлення DVB-T – 6817 несучих [2 – 5].

До основних переваг технології OFDM слід віднести стійкість до завмирань сигналу за умов багатопроменевості та високу спектральну ефективність [2, 3]. Багаточастотна структура групового сигналу зменшує чутливість системи передачі до імпульсних завад і дозволяє ефективно боротися із зосередженими за спектром завадами. Однак для OFDM-систем притаманні і свої проблеми [1 – 5]: одночасне випромінювання сигналу у всій смузі каналу, внаслідок чого зменшується радіус дії засобів зв'язку, а для збереження такої ж дальності дії, що і для одночастотних систем, необхідно збільшувати потужність передавача; високий пік-фактор; висока чутливість до помилок компенсації фазових зсувів в каналі, що порушує ортогональність несучих; високий рівень паразитної амплітудної модуляції, що вимагає підсилювача потужності з високою лінійністю характеристики; чутливість схеми до стабільності частоти. Для усунення впливу міжсимвольної інтерференції між символами OFDM вводиться захисний інтервал, який не дозволяє максимально ефективно використовувати виділений частотний ресурс (наприклад, для стандарту 802.11a коефіцієнт максимальної сумарної частотної ефективності складає 2,16 біт/(с·Гц)) [5].

Технологія OFDM являється перспективною і знайшла широке застосування в безпровідних мережах зв'язку цивільного призначення. Але системам військового радіозв'язку характерне функціонування при використанні противником навмисних завад. Аналіз характеристик навмисних завад, які можуть створювати сучасні комплекси та засоби радіоелектронного подавлення, показав, що особливу небезпеку для СРЗ з цифровою модуляцією представляють ретрансльовані та імітаційні дезінформуючі завади. Так американський наземний комплекс радіоелектронної боротьби для сухопутних військ «Вулфпак» за допомогою одного або декількох малогабаритних прийомо-передавальних пристроїв може здійснювати оптимальне подавлення ліній радіозв'язку спрямованими малопотужними завадами в результаті дії яких цифрові засоби радіозв'язку залишаються працездатними, але не забезпечують передачі корисної інформації [3].

Основними перевагами цього комплексу є: висока ефективність розкриття радіоелектронної обстановки; оптимальне подавлення ліній радіозв'язку і комплексів ППО супротивника цілеспрямованими малопотужними завадами без залучення традиційних засобів РЕП; можливість використання в режимі протидії засобам радіозв'язку (Р) і радіотехнічної розвідки (РТР) супротивника при веденні ними розвідки американських систем зв'язку і управління. З вищесказаного видно, що застосування OFDM сигналу при впливі навмисних завад ускладнено, та потребує вдосконалення [3].

Метою роботи є аналіз можливих шляхів вдосконалення засобів радіозв'язку з технологією OFDM при впливі навмисних завад

Для цього необхідно вирішити два головних напрямки:

1. Загальні методи (адаптивне формування діаграми направленості; адаптація до стану каналу зв'язку (КЗ), для цього необхідно вирішувати задачу оцінки стану каналу зв'язку; вибір вида сигнально-кодової конструкції (СКК) в підканалі).

2. Також для технології OFDM перспективним напрямком є додаткове розширення спектру з використанням технології CDMA (Code Division Multiple Access). При цьому виникає задача вибору ортогональних послідовностей для MC-CDMA систем. За допомогою розширювальної послідовності можливе зменшення пік-фактора (П) OFDM сигналів.

Адаптивне формування діаграми направленості

Важливим напрямком боротьби з завадами є просторова селекція, що полягає у застосуванні вузьконаправлених антен з яскраво вираженим основним пелюстком, і якомога більше подавленими боковими та заднім пелюстками. Даний спосіб можливо ефективно застосовувати для стаціонарних та пересувних засобів радіозв'язку середньої та великої потужності, в тому числі при ретрансляції інформаційних потоків.

Застосування адаптивних антенних решіток дозволяє антенній системі приймача точно налаштовуватися основним пелюстком діаграми направленості на кореспондента. При цьому бокові пелюстки намагаються зорієнтувати в тих напрямках, де шумовий фон найнижчий.

Додаткове розширення спектру

Одним з перспективним методів боротьби з навмисними завадами є розширення спектру за допомогою технології розширювальної кодових послідовностей (стандарти IMT-MC, CDMA-2000), CDMA основними принципами якої являється розширення спектра в поєднанні з кодовим розділенням фізичних каналів за рахунок використання псевдовипадкових послідовностей (ПВП).

Своєрідне поєднання технологій OFDM та CDMA створює технологію MC-CDMA (Multi Carrier Code Division Multiple Access). При формуванні MC-CDMA систем кожен біт потоку сигналів відображається на всі піднесучі, а кожна піднесуча використовує своє постійне в часі фазове зміщення, яке вибирається відповідно до заданого закону кодування. Ключова властивість системи MC-CDMA в тому, що всі чіпи, співставленні одному біту кода, передаються паралельно у вузькосмугових підканалах, з використанням MC-CDMA. Ця система володіє всіма перевагами OFDM та CDMA систем, та дозволяє боротися з частотно-селективними завмираннями і багатопроменевістю.

Зменшення впливу завад забезпечується наступними факторами:

По-перше, ефектом „розмивання" завад по спектру за рахунок перемноження прийнятої суміші сигналу і завади з ПВП.

По-друге, завадостійкість приймання OFDM-сигналу значно підвищується за рахунок підвищення стійкості пілот-сигналів (пілот-несучих) щодо впливу завад, що забезпечує більш точну оцінку поточного стану каналу зв'язку. Знання передаточної характеристики каналу, в свою чергу, дозволяє застосувати режекцію частини спектра, ураженої завадою, з відключенням передачі корисної інформації по відповідних піднесучих.

По-третє, якщо противник застосовує імітаційну заваду, яка в точності відтворює структуру сигналу, теоретично він не знає способу генерації ПВП. Тому така імітаційна завада хоч і буде створювати ефект внутрішньосистемних завад внаслідок неортогональності ПВП, що генеруються постановником завад і ЗРЗ, однак ефективність її значно зменшиться внаслідок узгодженої фільтрації після перемноження в кореляторі приймача.

Вибір виду розширювальної послідовності

Для розширення спектра в системах MC-CDMA використовуються різні види розширяючих послідовностей: двійкові (послідовності Уолша, послідовності Шапіро-Рудіна, коди Баркера, коди Голда, *M*-послідовності, послідовності Адамара) та багатофазні (послідовності Френка та Задова-Чу, послідовності Мілевського, послідовності Голея). Нижче розглянемо деякі найбільш ефективні послідовності, що використовуються в даний час.

Порівняльний аналіз цих послідовностей показав, що в системах MC-CDMA найменший пік-фактор забезпечують ідеальні багатофазні послідовності Френка, Задова-Чу, Мілевського ($П \leq 2$ (3дБ)). Двійкові послідовності Шапіро-Рудіна забезпечують $П \leq 4$ (6дБ). Недоліком вищеперелічених ідеальних послідовностей є те, що об'єм їх алфавіту збільшується зі зростанням числа піднесучих.

Також в [3] розглянуті 4-фазні послідовності Лі з одним нулем, ідеальні 8-фазні послідовності Люке с одним нулем та ідеальні 8-фазні послідовності з двома нулями. Ці послідовності також демонструють $\Pi \leq 2$ [8, 9].

Широке застосування в системах широкосмугового зв'язку знайшли так звані М-послідовності. Як правило, використовуються двійкові *М*-послідовності, символи яких $a(k)$ та $d(k)$ приймають значення $a(k)$ 1 та 0, $d(k)$ відповідно -1 та 1. Такі послідовності володіють наступними властивостями:

1) *М*-послідовність є періодичною с періодом $N = 2^n \quad 1$ символів, де N – кількість елементарних символів ПВП, а n – довільне ціле додатнє число;

2) кількість символів, які приймають значення одиниці, на довжині одного періода *М*-послідовності дорівнює $2^{n\ 1}$, що на одиницю більше, ніж кількість символів, що приймають значення нуль;

3) різні комбінації символів довжини n на довжині одного періода *М*-послідовності за винятком комбінації із n нулів зустрічаються не більш одного раза. Комбінація із n нулів являється забороненою, на її основі можлива генерація тільки послідовність із самих нулів;

4) сума по mod 2 любої *М*-послідовності з її довільним циклічним зсувом також є *М*-послідовністю;

5) періодична автокореляційна функція (АКФ) *М*-послідовності має постійний рівень бокових пелюстків, який дорівнює $(\ 1/N)$

Рівень максимальних бокових пелюстків аперіодичної АКФ приблизно складає $1/\sqrt{N}$.

Формування *М*-послідовності відбувається за допомогою багатократних лінійних фільтрів у вигляді регістрів зсуву з зворотнім зв'язком. Для формування М-послідовностей з періодом $N = 2^n \quad 1$ може використовуватись регістр зсуву довжиною n.

Коди Голда мають високе значення автокореляційної функції та низьке значення кореляції. Такі властивості забезпечують можливість використання цих кодів для реалізації множинного доступу с кодовим розділенням [8].

Коди Голда з періодом $2^n \quad 1$ формуються на основі двох *М*-послідовностей з відбором так званих "передаточних пар", які мають трьохзначну функцію автокореляції $(\ 1, \varphi(t), \varphi(t) \quad 2)$, де

$$\varphi(t) = \begin{cases} 2(N+1)/2, \text{ де } N \text{ парне}; \\ 2(N+2)/2, \text{ де } N \text{ непарне}. \end{cases} \qquad (1)$$

Коди Голда формуються шляхом суми кожного символу по модулю 2 двох m-послідовностей. Вони поділяються на три типа: первинні, вторинні ортогональні коди Голда (довжиною 256 біт) та довгий код.

Ортогональні коди Голда утворюються на основі *М*-послідовності довжиною 255 біт та добавлення одного надлишкового символу. Первинний синхрокод має аперіодичну автокореляційну функцію та використовується для початкового входу в синхронізм. Вторинний синхрокод представляє собою не модульований код Голда, який передається з первинним синхрокодом. Кожний вторинний синхрокод вибирається з 17 різних кодів Голда [8].

Оцінка стану каналу зв'язку

Завадостійкість приймання сигналів у сучасних системах радіозв'язку значною мірою залежить від точності оцінювання стану багатопроменевого каналу, який визначається його передаточною характеристикою і статистикою шуму [4]. При наявності інформації про стан каналу зв'язку при формуванні сигналу на передачі, прийомі та обробці – на прийомі, є можливість здійснювати заходи, спрямовані на підвищення показників завадостійкості та/або енергетичної ефективності СРЗ. Оцінка передаточної характеристики каналу зв'язку може

бути представлена як знаходження значень імпульсної характеристики каналу або відповідних їй значень частотної характеристики.

Розподіл потужності сигналу між підканалами OFDM системи

Також важливим фактором являється відключення найгірших за відношенням сигнал/шум піднесучих. Відключення піднесучих з низькими відношеннями сигнал/шум зменшує шкідливий вплив частотно-селективних завмирань на пропускну здатність і дозволяє перерозподілити потужність передавача між іншими піднесучих [7].

Вибір вида сигнально-кодової конструкції (СКК) в підканалі

Алгоритм вибору СКК для кожного власного каналу складається з вибору, в залежності від завадової обстановки, виду модуляції, вибору коректувального коду і вибору маніпуляційного коду.

Вибір виду модуляції. При створенні СКК широкий розвиток одержали методи двовимірної модуляції, при яких ансамблі сигналів можуть бути представлені крапками в двовимірному евклідовому просторі. Незважаючи на те, що теоретично при передачі інформації з каналу одномірні види модуляції мають такі ж потенційні можливості, що і двовимірні, при формуванні СКК одномірна модуляція використовується набагато рідше. Застосування багатомірних сигналів обмежується складністю реалізації таких СКК.

Більшість відомих СКК базується на використанні сигналів фазової маніпуляції (ФМ-*M*) і квадратурної амплітудної модуляції (КАМ-*M*) [7].

Вибір коректуючого коду. Важливим етапом побудови ефективних СКК є вибір методу захисту від помилок, що базуються на застосуванні завадостійких кодів. Використання цих кодів дозволяє отримати енергетичний виграш кодування (ЕВК), який характеризує ступінь можливого зниження енергетики передачі при кодуванні в порівнянні з відсутністю кодування, якщо достовірність передачі в обох випадках однакова. Цей виграш можна використовувати для поліпшення параметрів і характеристик багатьох важливих властивостей систем передачі даних, наприклад, для зменшення розмірів дуже дорогих антен, підвищення дальності зв'язку, збільшення швидкості передачі даних, зниження необхідної потужності передавача і т.д.

З [8] видно що найбільш ефективними на даний час коректуючими кодами є турбо і низькощільнісні коди. Кожен з них має свої переваги, недоліки і, відповідно, свою область застосування. Наприклад, турбо і низькощільнісні коди здатні працювати при рівні енергетики каналу, всього на декілька десятих децибела перевищуючих його пропускну здатність.

Застосування турбокодів при побудові СКК дозволило одержати додатковий енергетичний виграш відношення сигнал/шум для каналів із флуктуаційним шумом і завмираннями в порівнянні зі схемами, що використовують згорткові коди. Тому ці СКК на основі турбо кодів використовуються в багатьох сучасних комунікаційних засобах таких як стандарти без провідного доступу (БД) *IEEE*802.16*a,e* та *IEEE*802.11*n* [8].

Ймовірність помилки при застосуванні коригувального коду визначається виразом [5]

$$P_{\text{пом кк}} \approx \sum_{j=s_{\text{випр}}+1}^{n} C_n^j P_{\text{пом}}^j (1 - P_{\text{пом}})^{n-j}, \qquad (2)$$

де $P_{\text{пом кк}}$ – ймовірність помилкового декодування кодової комбінації, $s_{\text{випр}} = (d - 1)/2$ – кратність помилок, яку код виправляє, j – кратність помилки у блоці з n елементів, $P_{\text{пом}}$ – ймовірність виникнення помилок в послідовності переданих кодових елементів,

$C_n^j = n!/j!(n\ \ j)!$ – біноміальний коефіцієнт, який дорівнює кількості різних сполучень j помилок у блоці з n символів.

Вибір маніпуляційного коду. При узгодженні кодека двійкового завадостійкого коду і модему багатопозиційних сигналів, необхідно використовувати маніпуляційний код, при якому більшій відстані за Хеммінгом між кодовими комбінаціями відповідає більша відстань за Евклідом між сигналами, що їм відповідають.

Способи узгодження модуляції і кодування можна розділити на двох груп: узгодження оптимальним маніпуляційним кодом і узгодження на основі розбиття ансамблю на вкладені підансамблі.

СКК, що відносяться до першої групи, є результатом узгодження відомих двійкових завадостійких кодів із багатопозиційним ансамблем сигналів шляхом використання спеціальним чином підібраного маніпуляційного коду. Оскільки помилки найчастіше відбуваються за рахунок переходів в області сусідніх сигналів, то кодові комбінації, які відповідають сусіднім сигналам, повинні розрізнятися найменшою кількістю двійкових символів. Цій вимозі в ряді випадків задовольняє код Грея [3, 8].

Друга група включає досить велику кількість типів СКК, які розрізняються модифікаціями методів узгодження. Основою побудови СКК такого виду є розбиття ансамблю сигналів на вкладені підансамблі [3, 7]. Розбиття здійснюється таким чином, що підансамблі мають однакову кількість сигнальних точок. Відстані d_E між сусідніми сигналами підансамблів однакові, а мінімальні відстані $d_{E\min}$ між сигналами підансамблю збільшуються з кожним кроком розбиття.

Отже, основним напрямком вдосконалення технології OFDM в умовах навмисних завад являється додаткове розширення спектра сигналу за допомогою поєднання технологій OFDM і CDMA, яке створює технологію MC-CDMA (Multi Carrier Code Division Multiple Access).

Основними проблемами, при використанні технологію MC-CDMA, являється оцінка стану каналу зв'язку, вибір виду розширяючої послідовності, вибір параметрів розширяючої послідовності, розподіл потужності сигналу між підканалами OFDM сигналу та вибір виду СКК в підканалі.

Список літератури

1. *Григорьев В. А.* Сети и системы радиодоступа / В. А. Григорьев, О. И. Лагутенко, Ю. А. Распаев // М.: Око-Трендз, 2005. – 384 с.

2. *Вишневский В. М.* Широкополосные беспроводные сети передачи информации / В. М. Вишневский, А. И. Ляхов, С. Л. Портной, И. В. Шахнович // – М.: Техносфера, 2005. – 592 с.

3. *Кувшинов О.В.* Технологія OFDM: огляд проблем та шляхів їх розв'язання О.В Кувшинов, Т.Г. Гурський // Зв'язок. – 2008. – №. 1 (77). – С. 42-46.

4. *Міночкін Д.А.* Метод контролю стану каналу зв'язку із селективними завмираннями / Д.А. Міночкін, І. В. Борисов. // Збірник наукових праць ВІТІ НТУУ „КПІ". – 2006. – Вип. 3. – С. 66–71.

5. *Кувшинов О.В.* Теорія електричного зв'язку. Ч. 2: Основи теорії завадостійкості, кодування та інформації / О.В. Кувшинов, С.П. Лівенцев, О.П. Лежнюк, А.І. Міночкін, Д.І. Могилевич // Підручник. – К.: ВІТІ НТУУ «КПІ», 2008. – 286 с

6. *Голяницкий И.А.* Математические модели и методы в радиосвязи / И.А. Голяницкий // Под ред. Ю.А. Громакова. – М: Эко-Трендз, 2005. – 440 с.

7. *Кувшинов О. В.* Методика вибору сигнально-кодових конструкцій в системах рухомого радіозв'язку О.В. Кувшинов. // Зв'язок. – 2002. – № 3. – С. 30-34.

8. R. van Nee and R. Prasad, OFDM for Wireless Multimedia Communications, Artech, 2000.

9. *L.Hanzo.* OFDM and MC-CDMA for Broadband multi-User Communications, WLANs and Broadcating, John Wiley&Sons,Ltd., 2003.

Рецензент: Лєнков С.В..
Надійшла 6.10.2011