УДК 621.391

С.В. ЗАЙЦЕВ, А.В. ЯРИЛОВЕЦЬ, В.Д. НАЗАРУК

ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПОБУДОВИ СИСТЕМИ OFDM-FHSS НА ОСНОВІ ОПТИМАЛЬНИХ ЧАСТОТНО-ЧАСОВИХ СИГНАЛЬНО-КОДОВИХ КОНСТРУКЦІЙ

Анотація. *У статті розроблена інформаційна технологія побудови системи OFDM-FHSS на основі оптимальних частотно-часових послідовностей та кодів Рида-Соломона. Використання розробленої інформаційної технології на практиці дозволить підвищити завадостійкість та зменшити складність реалізації засобів радіозв'язку, які використовують технологію OFDM-FHSS.*
Ключові слова: *технологія OFDM-FHSS, коди Рида-Соломона.*

Аннотация. *В статье разработана информационная технология построения системы OFDM-FHSS на основе оптимальных частотно-временных последовательностей и кодов Рида-Соломона. Использование разработанной информационной технологии на практике позволит повысить помехоустойчивость и уменьшить сложность реализации средств радиосвязи, использующих технологию OFDM-FHSS.*
Ключевые слова: *технология OFDM-FHSS, коды Рида-Соломона.*

Abstract. *Information technology of OFDM-FHSS system construction based on optimal time-frequency sequences and Reed-Solomon codes was designed in the paper. The usage of developed information technology in practice will improve noise immunity and reduce the complexity of radio communications used OFDM-FHSS technology.*
Keywords: *OFDM-FHSS technology, Reed-Solomon codes.*

1. Вступ

На сьогоднішній день фізичний рівень мобільних систем радіозв'язку ґрунтується на використанні технології ортогонально-частотного мультиплексування OFDM (Orthogonal frequency-division multiplexing), технології швидкої стрибкоподібної зміни частоти FHSS (Frequency Hopping Spread Spectrum), технології CDMA (Code Division Multiple Access) та використанні завадостійкого кодування [1–3].

Для забезпечення процесу передавання повідомлень кожна пара приймач і передавач сигналу OFDM-FHSS повинні використовувати однакові закони зміни частот [1]. Застосування законів зміни частоти за псевдовипадковим законом значно ускладнює визначення цього закону, до того ж підвищується розвідзахищеність і ускладнюється можливість перехоплення інформації [4, 5]. Це є наслідком того, що для здійснення відновлення переданого повідомлення на фізичному рівні необхідно виконати демодуляцію перехопленого радіосигналу. А це досить складна задача, якщо псевдовипадкові частотно-часові коди невідомі. Закон формування частотно-часових послідовностей (ЧЧП), що визначає послідовність слідування несучих частот сигналу OFDM-FHSS, повинен бути псевдовипадковим. Однак алгоритм формування цих послідовностей має бути досить простим для того, щоб забезпечити нормальне функціонування цифрових формувачів сигналу OFDM-FHSS. При цьому, виходячи з потреб захисту інформації, необхідно забезпечити можливість досить швидкої зміни номера цієї псевдовипадкової послідовності і в процесі передавання інформації.

2. Постановка задачі

Якщо взяти $N = M + 1$ – просте число, де M – кількість частот у сигналі OFDM-FHSS, то можливо побудувати $N - 1$ оптимальних ЧЧП. При цьому під оптимальними розуміємо ортогональні ЧЧП, у яких при довільних часових зсувах співпадає не більше одного частотно-часового елемента. Для підвищення завадозахищеності системи OFDM-FHSS з оптимальними ЧЧП необхідно використовувати завадостійке кодування. Як завадостійкі коди можна використати коди Рида-Соломона.

Таким чином, виникає завдання розробки інформаційної технології побудови системи OFDM-FHSS на основі оптимальних частотно-часових послідовностей та кодів Рида-Соломона.

Метою роботи є розробка інформаційної технології побудови системи OFDM-FHSS на основі оптимальних частотно-часових сигнально-кодових конструкцій.

3. Виклад основного матеріалу

Система OFDM-FHSS на основі оптимальних частотно-часових сигнально-кодових конструкцій складається з передавальної та приймальної частин. Передавальна та приймальна частини мають у своєму складі такі елементи: кодер (декодер) Рида-Соломона, модулятор (демодулятор) OFDM-FHSS на основі оптимальних ЧЧП.

На рис. 1, 2 показана спрощена структурна схема архітектури передачі та прийому фізичного рівня радіозасобів з технологією OFDM-FHSS та коригувальними кодами Рида-Соломона.

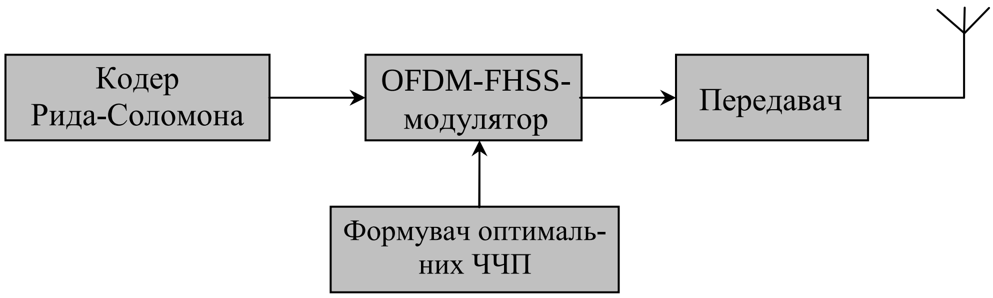

Рис. 1. Структурна схема архітектури передачі фізичного рівня радіозасобів з технологією OFDM-FHSS та коригувальними кодами Рида-Соломона

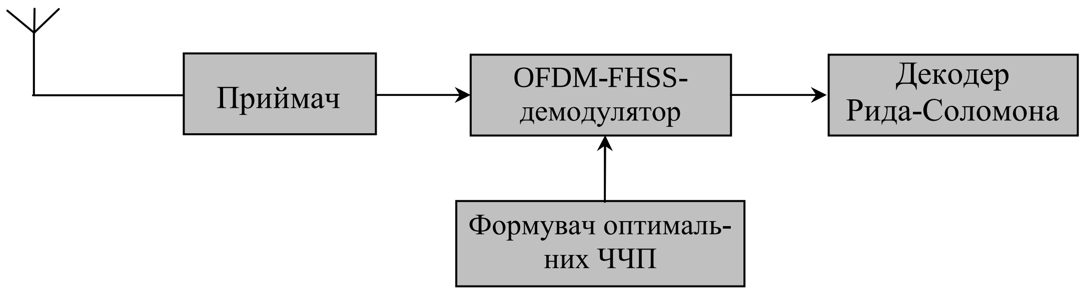

Рис. 2. Структурна схема архітектури прийому фізичного рівня радіозасобів з технологією OFDM-FHSS та коригувальними кодами Рида-Соломона

Основна ідея методу OFDM полягає в тому, що смуга пропускання каналу розбивається на групу вузьких смуг (субканалів), кожна зі своєю піднесучою. На всіх піднесучих сигнал передається одночасно, що дозволяє забезпечити велику швидкість передачі інформації при невеликій швидкості передачі в кожному окремому субканалі [1]. Сигнал OFDM складається із N ортогональних піднесучих, модульованих N паралельними потоками даних.

Формування підканалів з ортогональними піднесучими відбувається за допомогою процедури зворотного дискретного перетворення Фур'є (ДПФ) [1]. На практиці процедури зворотного ДПФ (на передаючій стороні) та прямого ДПФ (на прийомній) реалізуються за допомогою алгоритму швидкого перетворення Фур'є (ШПФ) та виконуються процесором ШПФ [1, 2].

Структурна схема модулятора сигналу OFDM, каналу з адитивним білим гаусівським шумом та демодулятора сигналу OFDM показана на рис. 3.

Таким чином, функції OFDM-модулятора зводяться до формування складового неперервного сигналу, який містить N піднесучих, більша частина з яких модульовані інформаційними символами на інтервалі T_s [1]:

$$s(t)=\sum_{k=0}^{N-1} X(k) e^{j2\pi k\Delta f t}, \tag{1}$$

де N – кількість піднесучих, $X(k)$ – комплексний модулюючий символ (ФМ-*M* або КАМ-*M*), який передається на k-й піднесучій $e^{j2\pi k\Delta f t}$, $\Delta f=1/T_s$ – частота слідування символів, T_s – тривалість символу.

Реалізація функцій OFDM-модулятора на базі цифрового процесора ШПФ передбачає перехід від безперервного часу до дискретного $(t=nT)$, при цьому вираз (1), з урахуванням періоду дискретизації $T=T_S/N$, прийме вигляд [1]

$$s(\frac{n}{N}T_s)=\sum_{k=0}^{N-1} X(k) e^{j2\pi k\frac{n}{N}},\ n=\overline{0, N-1}. \tag{2}$$

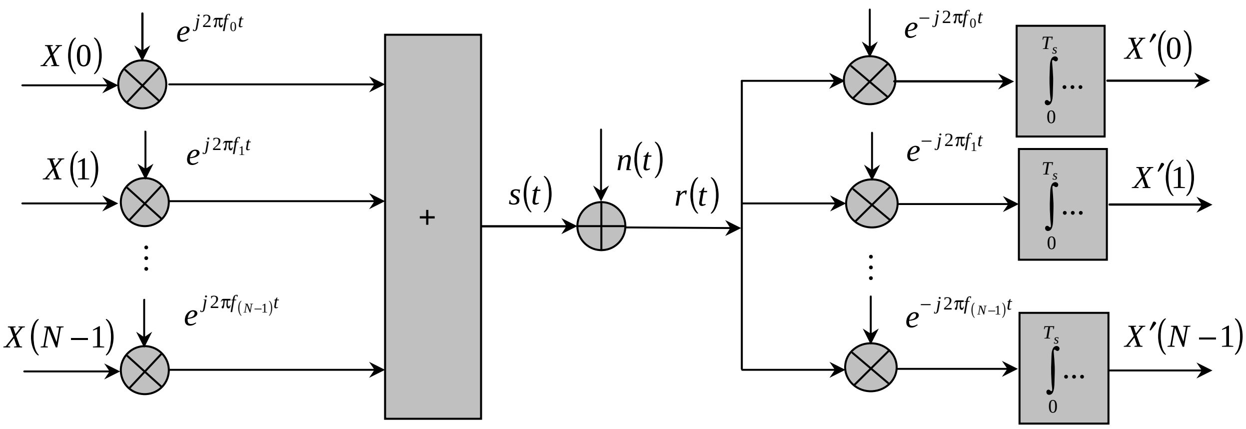

Рис. 3. Структурна схема моделі модулятора сигналу OFDM, каналу з АБГШ та демодулятора сигналу OFDM

Можна представити $s\left(\frac{n}{N}T_s\right)$ як залежність від n, $s(n)$ і тоді (2) представимо як

$$s(n)=W^{-1}X(k),\ k,n=\overline{0, N-1}), \tag{3}$$

де W – це матриця розміру $N\times N$ дискретного перетворення Фур'є з елементами

$$[W]_{k,n}=e^{-j2\pi kn/N},\ k,n=\overline{0,(N-1)},$$

$$W = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & e^{-j2\pi/N} & e^{-j4\pi/N} & \cdots & e^{-j2\pi(N-1)/N} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & e^{-j2\pi(N-2)/N} & e^{-j4\pi(N-2)/N} & \cdots & e^{-j2\pi(N-1)(N-2)/N} \\ 1 & e^{-j2\pi(N-1)/N} & e^{-j4\pi(N-1)/N} & \cdots & e^{-j2\pi(N-1)(N-1)/N} \end{bmatrix}.$$

На приймальній стороні відбуваються такі перетворення:

$$X'(n) = \frac{1}{T_s}\int_0^{T_s}\left[s(t)+n(t)\right]e^{-j2\pi n\Delta ft}dt,\ n=\overline{0,N-1}.$$

Оптимальний алгоритм знаходження елементів матриці номерів частот визначається таким виразом:

$$[\Psi]_{k,n} = (k\times n)\operatorname{mod}(M+1), k,n=\overline{0,(N-1)},$$

де k – номер строки, n – номер стовпця. При визначенні (2) було враховано, що $A\cdot \operatorname{mod}(B) = A-(A\div B)$, де „$\div$” – операція ділення без залишку (націло). Не важко переконатися, що, завдяки формулі (7), значно спрощується знаходження оптимальних алфавітів для формування сигналу OFDM.

Наприклад, при $N=12$ матриця номерів частот буде мати такий вигляд:

$$[\Psi]_{k,n} = \begin{vmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 5 & 6 & 8 & 9 & 10 & 11 \\ 1 & 3 & 5 & 7 & 9 & 11 & 0 & 2 & 4 & 6 & 8 & 10 \\ 2 & 5 & 8 & 11 & 1 & 4 & 7 & 10 & 0 & 3 & 6 & 9 \\ 3 & 7 & 11 & 2 & 6 & 10 & 1 & 5 & 9 & 0 & 4 & 8 \\ 4 & 9 & 1 & 6 & 11 & 3 & 8 & 0 & 5 & 10 & 2 & 7 \\ 5 & 11 & 4 & 10 & 3 & 9 & 2 & 8 & 1 & 7 & 0 & 6 \\ 6 & 0 & 7 & 1 & 8 & 2 & 9 & 3 & 10 & 4 & 11 & 5 \\ 7 & 2 & 10 & 5 & 0 & 8 & 3 & 11 & 6 & 1 & 9 & 4 \\ 8 & 4 & 0 & 9 & 5 & 1 & 10 & 6 & 2 & 11 & 7 & 3 \\ 9 & 6 & 3 & 0 & 10 & 7 & 4 & 1 & 11 & 8 & 5 & 2 \\ 10 & 8 & 6 & 4 & 2 & 0 & 11 & 9 & 7 & 5 & 3 & 1 \\ 11 & 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & 0 \end{vmatrix}.$$

У результаті сигнал OFDM з оптимальним алгоритмом знаходження елементів матриць номерів частот можна представити так:

$$s(n) = e^{-j2\pi n[\Psi]_{k,n}/N}X(k),\ \ k,n=\overline{0,N-1}). \tag{4}$$

Коди Рида-Соломона (Reed-Solomon code, R-S code) [6] – це недвійкові циклічні коди, символи яких являють собою m бітові послідовності, де m – позитивне ціле число, більше 1. Коди Рида-Соломона (n,k) визначені на m-бітових символах при всіх n та k, для яких

$$0<k<n<2^m+2, \tag{5}$$

де k – число інформаційних бітів, які підлягають кодуванню, n – число кодових символів у блоці, який кодується.

Так як код Рида-Соломона є циклічним, кодування в систематичній формі аналогічно процедурі двійкового кодування. Ми можемо здійснити зсув полінома повідомлення $m(X)$ у крайні праві k-розряди регістра кодового слова та зробити наступний додаток полінома $p(X)$ у крайні ліві $n-k$ розряди. Тому ми множимо $m(X)$ на X^{n-k}, проробивши алгебраїчну операцію таким чином, що $m(X)$ виявляється зсуненим вправо на $n-k$ позицій. Далі ми ділимо $X^{n-k}m(X)$ на поліноміальний генератор $g(X)$, що можна записати таким способом:

$$X^{n-k}m(X) = q(X)g(X) + p(X). \tag{6}$$

Тут $q(X)$ і $p(X)$ – це частка та залишок від поліноміального ділення. Як і у випадку двійкового кодування, залишок буде парним. Рівняння (6) можна переписати таким чином:

$$p(X) = X^{n-k}m(X) \text{ по модулю } g(X). \tag{7}$$

Результуючий поліном кодового слова $U(X)$ можна переписати таким чином:

$$U(X) = p(X) + X^{n-k}m(X). \tag{8}$$

Продемонструємо кроки, які маються на увазі, рівняннями (7) і (8), закодувавши повідомлення із трьох символів:

$$\underbrace{010}_{\alpha^1}\underbrace{110}_{\alpha^3}\underbrace{111}_{\alpha^5}$$

за допомогою коду Рида-Соломона (7, 3), генератор якого визначається рівнянням $g(X) = \alpha^3 + \alpha^1 X + \alpha^0 X^2 + X^4$. Спочатку ми множимо (зсув вверх) поліном повідомлення $\alpha^1 + \alpha^3 X + \alpha^5 X^2$ на $X^{n-k} = X^4$, що дає $\alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$.

Далі ми ділимо такий зсунутий вверх поліном повідомлення на поліноміальний генератор з рівняння $\alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6$, $\alpha^3 + \alpha^1 X + \alpha^0 X^2 + X^4$.

Операції додавання (вирахування) і множення (ділення) при поліноміальному діленні недвійкових коефіцієнтів виконуються відповідно до табл. 1 та 2.

Таблиця 1. Таблиця додавання для GF(8) для $f(X) = 1 + X + X^3$

	$\boldsymbol{\alpha^0}$	$\boldsymbol{\alpha^1}$	$\boldsymbol{\alpha^2}$	$\boldsymbol{\alpha^3}$	$\boldsymbol{\alpha^4}$	$\boldsymbol{\alpha^5}$	$\boldsymbol{\alpha^6}$
$\boldsymbol{\alpha^0}$	0	α^3	α^6	α^1	α^5	α^4	α^2
$\boldsymbol{\alpha^1}$	α^3	0	α^4	α^0	α^2	α^6	α^5
$\boldsymbol{\alpha^2}$	α^6	α^4	0	α^5	α^1	α^3	α^0
$\boldsymbol{\alpha^3}$	α^1	α^0	α^5	0	α^6	α^2	α^4
$\boldsymbol{\alpha^4}$	α^5	α^2	α^1	α^6	0	α^0	α^3
$\boldsymbol{\alpha^5}$	α^4	α^6	α^3	α^2	α^0	0	α^1
$\boldsymbol{\alpha^6}$	α^2	α^5	α^0	α^4	α^3	α^1	0

Таблиця 2. Таблиця множення для GF(8) для $f(X) = 1 + X + X^3$

	$\boldsymbol{\alpha^0}$	$\boldsymbol{\alpha^1}$	$\boldsymbol{\alpha^2}$	$\boldsymbol{\alpha^3}$	$\boldsymbol{\alpha^4}$	$\boldsymbol{\alpha^5}$	$\boldsymbol{\alpha^6}$
$\boldsymbol{\alpha^0}$	α^0	α^1	α^2	α^3	α^4	α^5	α^6
$\boldsymbol{\alpha^1}$	α^1	α^2	α^3	α^4	α^5	α^6	α^0

Продовж. табл. 2

$\boldsymbol{\alpha^2}$	α^2	α^3	α^4	α^5	α^6	α^0	α^1
$\boldsymbol{\alpha^3}$	α^3	α^4	α^5	α^6	α^0	α^1	α^2
$\boldsymbol{\alpha^4}$	α^4	α^5	α^6	α^0	α^1	α^2	α^3
$\boldsymbol{\alpha^5}$	α^5	α^6	α^0	α^1	α^2	α^3	α^4
$\boldsymbol{\alpha^6}$	α^6	α^0	α^1	α^2	α^3	α^4	α^5

У результаті поліноміальне ділення дасть такий поліноміальний залишок (поліном парності):

$$p(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3. \tag{9}$$

Потім з рівняння (8) поліном кодового слова можна записати таким способом:

$$U(X) = \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^6 X^3 + \alpha^1 X^4 + \alpha^3 X^5 + \alpha^5 X^6 =$$

$$= (100) + (001)X + (011)X^2 + (101)X^3 + (010)X^4 + (110)X^5 + (111)X^6. \tag{10}$$

Тестове повідомлення кодується в систематичній формі за допомогою коду Рида-Соломона (7, 3), що у результаті дасть поліном кодового слова, який описується рівнянням (10). Допустимо, що в ході передачі це кодове слово піддалося перекручуванню: 2 символи були прийняті з помилкою. При використанні 7-символьного кодового слова модель помилки можна представити в поліноміальній формі таким способом:

$$e(X) = \sum_{n=0}^{6} e_n X^n. \tag{11}$$

Нехай двохсимвольна помилка буде такою, що

$$e(X) = 0 + 0X + 0X^2 + \alpha^2 X^3 + \alpha^5 X^4 + 0X^5 + 0X^6 =$$

$$= (000) + (000)X + (000)X^2 + (001)X^3 + (111)X^4 + (000)X^5 + (000)X^6. \tag{12}$$

Інакше кажучи, контрольний символ зіпсований 1-бітовою помилкою (представленою як α^2, а символ повідомлення – 3-бітовою помилкою (представленою як α^5). У цьому випадку прийнятий поліном зіпсованого кодового слова $r(X)$ представляється у вигляді суми полінома переданого кодового слова та полінома моделі помилки, як показано нижче:

$$r(X) = U(X) + e(X). \tag{13}$$

Дотримуючись рівняння (13), підсумуємо $U(X)$ з рівняння (10) і $e(X)$ з рівняння (12). Отже, маємо

$$r(X) = (100) + (001)X + (011)X^2 + (100)X^3 + (101)X^4 + (110)X^5 + (111)X^6 =$$

$$= \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^6 X^4 + \alpha^3 X^5 + \alpha^5 X^6. \tag{14}$$

У даному прикладі виправлення 2-символьної помилки є чотири невідомих – два ставляться до розташування помилки, а два стосуються помилкових значень. При двійковому декодуванні декодеру потрібно знати лише розташування помилки. Якщо відомо, де перебуває помилка, біт потрібно поміняти з 1 на 0 або навпаки. Але тут недвійкові символи вимагають, щоб ми не тільки довідалися розташування помилки, але й визначили правильне значення символу, розташованого на цій позиції. Оскільки в даному прикладі у нас є чотири невідомих, нам потрібно чотири рівняння, щоб знайти їх.

Синдром – це результат перевірки парності, виконуваної над r, щоб визначити, чи належить r набору кодових слів. Якщо r є членом набору, то синдром S має значення, рівне 0. Будь-яке ненульове значення S означає наявність помилок. Так само, як і у двійковому випадку, синдром S складається з $n-k$ символів, $\{S_i\}$, $i=\overline{1,n-k}$. Таким чином, для нашого коду (7, 3) є по чотирі символи в кожному векторі синдрому; їх значення можна розрахувати із прийнятого полінома $r(X)$. Помітимо, як полегшуються обчислення завдяки самій структурі коду, обумовленої рівнянням

$$U(X)=m(X)g(X). \tag{15}$$

З цієї структури можна бачити, що кожен правильний поліном кодового слова $U(X)$ є кратним поліноміальному генератору $g(X)$. Отже, корні $g(X)$ також повинні бути коренями $U(X)$. Оскільки $r(X)=U(X)+e(X)$, то $r(X)$, що обчислюється з кожним коренем $g(X)$, повинен давати нуль, тільки якщо $r(X)$ буде правильним кодовим словом. Будь-які помилки приведуть у підсумку до ненульового результату в одному (або більше) випадку. Обчислення символів синдрому можна записати таким способом:

$$S_i=r(X)\Big|_{X=\alpha^i}=r(\alpha^i),\ \ i=\overline{1,n-k}. \tag{16}$$

Тут, як було показано в рівнянні (12), $r(X)$ містить 2-символьні помилки. Якщо $r(X)$ виявиться правильним кодовим словом, то це приведе до того, що всі символи синдрому S будуть дорівнювати нулю. У даному прикладі чотири символи синдрому знаходяться таким способом:

$$S_1=r(\alpha)=\alpha^0+\alpha^3+\alpha^6+\alpha^3+\alpha^{10}+\alpha^8+\alpha^{11}=$$
$$=\alpha^0+\alpha^3+\alpha^6+\alpha^3+\alpha^2+\alpha^8+\alpha^4=\alpha^3, \tag{17}$$

$$S_2=r(\alpha^2)=\alpha^0+\alpha^4+\alpha^8+\alpha^6+\alpha^{14}+\alpha^{13}+\alpha^{17}=$$
$$=\alpha^0+\alpha^4+\alpha^1+\alpha^6+\alpha^0+\alpha^6+\alpha^3=\alpha^5, \tag{18}$$

$$S_3=r(\alpha^3)=\alpha^0+\alpha^5+\alpha^{10}+\alpha^9+\alpha^{18}+\alpha^{18}+\alpha^{23}=$$
$$=\alpha^0+\alpha^5+\alpha^3+\alpha^2+\alpha^4+\alpha^4+\alpha^2=\alpha^6, \tag{19}$$

$$S_4=r(\alpha^4)=\alpha^0+\alpha^6+\alpha^{12}+\alpha^{12}+\alpha^{22}+\alpha^{23}+\alpha^{29}=$$
$$=\alpha^0+\alpha^6+\alpha^5+\alpha^5+\alpha^1+\alpha^2+\alpha^1=0. \tag{20}$$

Результат підтверджує, що прийняте кодове слово містить помилку (введену нами), оскільки $S\neq 0$.

Припустимо, що у кодовому слові є v помилок, розташованих на позиціях $X^{j_1}, X^{j_2},..., X^{j_v}$. Тоді поліном помилок, обумовлений рівняннями (11) і (12), можна записати таким способом:

$$e(X)=e_{j_1}X^{j_1}+e_{j_2}X^{j_2}+...+e_{j_v}X^{j_v}. \tag{21}$$

Індекси 1, 2, ..., v позначають 1-у, 2-у, ..., $v-y$ помилки, а індекс j – розташування помилки. Для корекції перекрученого кодового слова потрібно визначити кожне значення помилки e_{j_l} і її розташування X^{j_l}, де $l = \overline{1,v}$. Позначимо номер локатора помилки як $\beta_l = \alpha^{j_l}$. Далі обчислюємо $n - k = 2t$ символи синдрому, підставляючи α у прийнятий поліном при $i = 1, 2, \ldots, 2t$.

$$\begin{gathered} S_1 = r(\alpha) = e_{j_1}\beta_1 + e_{j_2}\beta_2 + \ldots + e_{j_v}\beta_v, \\ S_2 = r(\alpha^2) = e_{j_1}\beta_1^2 + e_{j_2}\beta_2^2 + \ldots + e_{j_v}\beta_v^2, \\ \vdots \\ S_{2t} = r(\alpha^{2t}) = e_{j_1}\beta_1^{2t} + e_{j_2}\beta_2^{2t} + \ldots + e_{j_v}\beta_v^{2t}. \end{gathered} \tag{22}$$

У нас є $2t$ невідомих (t значень помилок і t розташувань) і система $2t$ рівнянь. Але цю систему $2t$ рівнянь не можна вирішити звичайним шляхом, оскільки рівняння в ній нелінійні (деякі невідомі входять у рівняння в ступені). Методика, що дозволяє вирішити цю систему рівнянь, називається алгоритмом декодування Рида-Соломона.

Якщо обчислено ненульовий вектор синдрому (один або більше його символів не дорівнюють нулю), це означає, що була прийнята помилка. Далі потрібно довідатися розташування помилки (або помилок). Полином локатора помилок можна визначити таким способом:

$$\begin{aligned} \sigma(X) &= (1+\beta_1 X)(1+\beta_2 X)\ldots(1+\beta_v X) = \\ &= 1 + \sigma_1 X + \sigma_2 X^2 + \ldots + \sigma_v X^v. \end{aligned} \tag{23}$$

Коренями $\sigma(X)$ будуть $1/\beta_1, 1/\beta_2, \ldots, 1/\beta_v$. Величини, зворотні кореням $\sigma(X)$, будуть представляти номери розташувань моделей помилки $e(X)$. Тоді, скориставшись авторегресійною технікою моделювання, ми складемо із синдромів матрицю, в якій перші t синдромів будуть використовуватися для передбачення наступного синдрому:

$$\begin{bmatrix} S_1 & S_2 & S_3 & \cdots & S_{t-1} & S_t \\ S_2 & S_3 & S_4 & \cdots & S_t & S_{t+1} \\ & & & \vdots & & \\ S_{t-1} & S_t & S_{t+1} & \cdots & S_{2t-3} & S_{2t-2} \\ S_t & S_{t+1} & S_{t+2} & \cdots & S_{2t-2} & S_{2t-1} \end{bmatrix} \begin{bmatrix} \sigma_t \\ \sigma_{t-1} \\ \vdots \\ \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{2t-1} \\ -S_{2t} \end{bmatrix}. \tag{24}$$

Ми скористалися авторегресійною моделлю рівняння (24), взявши матрицю найбільшої розмірності з ненульовим визначником. Для коду (7, 3) з корекцією двохсимвольних помилок матриця буде мати розмірність 2x2 і модель запишеться таким способом:

$$\begin{bmatrix} S_1 & S_2 \\ S_2 & S_3 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} S_3 \\ S_4 \end{bmatrix}, \tag{25}$$

$$\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} \begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^6 \\ 0 \end{bmatrix}. \tag{26}$$

Щоб знайти коефіцієнти σ_1 й σ_2 полінома локатора помилок $\sigma(X)$, спочатку необхідно обчислити зворотну матрицю для рівняння (26). Зворотна матриця для матриці $[A]$ визначається таким способом:

$$Inv[A] = \frac{cofactor[A]}{\det[A]}. \tag{27}$$

Отже,

$$\det\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} = \alpha^3\alpha^6 - \alpha^5\alpha^5 = \alpha^9 + \alpha^{10} = \alpha^2 + \alpha^3 = \alpha^5, \tag{28}$$

$$cofactor\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} = \begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix}, \tag{29}$$

$$Inv\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix} = \frac{\begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix}}{\alpha^5} = \alpha^{-5}\begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix} =$$

$$= \alpha^2\begin{bmatrix} \alpha^6 & \alpha^5 \\ \alpha^5 & \alpha^3 \end{bmatrix} = \begin{bmatrix} \alpha^8 & \alpha^7 \\ \alpha^7 & \alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & \alpha^5 \end{bmatrix}. \tag{30}$$

Якщо зворотна матриця обчислена правильно, то добуток вихідної й зворотної матриці повинен дати одиничну матрицю:

$$\begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix}\begin{bmatrix} \alpha^1 & \alpha^0 \\ \alpha^0 & \alpha^5 \end{bmatrix} = \begin{bmatrix} \alpha^4 + \alpha^5 & \alpha^3 + \alpha^{10} \\ \alpha^6 + \alpha^6 & \alpha^5 + \alpha^{11} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}. \tag{31}$$

За допомогою рівняння (26) почнемо пошук положень помилок з обчислення коефіцієнтів полінома локатора помилок $\sigma(X)$, як показано далі:

$$\begin{bmatrix} \sigma_2 \\ \sigma_1 \end{bmatrix} = \begin{bmatrix} \alpha^3 & \alpha^5 \\ \alpha^5 & \alpha^6 \end{bmatrix}\begin{bmatrix} \alpha^6 \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha^7 \\ \alpha^6 \end{bmatrix}\begin{bmatrix} \alpha^0 \\ \alpha^6 \end{bmatrix}. \tag{32}$$

З рівнянь (32) і (33)

$$\sigma(X) = \alpha^0 + \sigma_1 X + \sigma_2 X^2 = \alpha^0 + \alpha^6 X + \alpha^0 X^2. \tag{33}$$

Корені $\sigma(X)$ є оберненими числами до положень помилок. Після того, як ці корені знайдені, ми знаємо розташування помилок. Взагалі, корені $\sigma(X)$ можуть бути одним або декількома елементами поля. Визначимо ці корені шляхом повної перевірки полінома $\sigma(X)$ з усіма елементами поля, як буде показано нижче. Будь-який елемент X, який дає $\sigma(X) = 0$, є коренем, що дозволяє нам визначити розташування помилки.

$$\begin{aligned}
\sigma(\alpha^0) &= \alpha^0 + \alpha^6 + \alpha^0 = \alpha^6 \neq 0 \\
\sigma(\alpha^1) &= \alpha^2 + \alpha^7 + \alpha^0 = \alpha^2 \neq 0 \\
\sigma(\alpha^2) &= \alpha^4 + \alpha^8 + \alpha^0 = \alpha^6 \neq 0 \\
\sigma(\alpha^3) &= \alpha^6 + \alpha^9 + \alpha^0 = 0 \Rightarrow \textit{Помилка} \\
\sigma(\alpha^4) &= \alpha^8 + \alpha^{10} + \alpha^0 = 0 \Rightarrow \textit{Помилка} \\
\sigma(\alpha^5) &= \alpha^{10} + \alpha^{11} + \alpha^0 = \alpha^2 \neq 0 \\
\sigma(\alpha^6) &= \alpha^{12} + \alpha^{12} + \alpha^0 = \alpha^0 \neq 0
\end{aligned}.$$

Як видно з рівняння (23), розташування помилок є зворотною величиною до коренів полінома. А, значить, $\sigma(\alpha^3)=0$ означає, що один корінь отримується при $1/\beta_l=\alpha^3$. Звідси $\beta_l=1/\alpha^3=\alpha^4$. Аналогічно $\sigma(\alpha^4)=0$ означає, що інший корінь з'являється при $1/\beta_{l'}=1/\alpha^4=\alpha^3$, де (у даному прикладі) l та l' позначають 1-у і 2-у помилки. Оскільки ми маємо справу з 2-символьними помилками, поліном помилок можна записати таким чином:

$$e(X)=e_{j_1}X^{j_1}+e_{j_2}X^{j_2}. \tag{34}$$

Тут були знайдені дві помилки на позиціях α^3 і α^4. Помітимо, що індексація номерів розташування помилок є сугубо довільною. Отже, у цьому прикладі ми позначили величини $\beta_l=\alpha^{j_l}$ як $\beta_1=\alpha^{j_1}=\alpha^3$ і $\beta_2=\alpha^{j_2}=\alpha^4$.

Ми позначили помилки e_{j_l}, де індекс j позначає розташування помилки, а індекс l – l-у помилку. Оскільки кожне значення помилки пов'язане з конкретним місцем розташування, систему позначень можна спростити, позначивши e_{j_l} просто як e_l. Тепер, приготувавшись до знаходження значень помилок e_1 і e_2, пов'язаних з позиціями $\beta_1=\alpha^3$ та $\beta_2=\alpha^4$, можна використати кожне із чотирьох синдромних рівнянь. Виразимо з рівняння (11) S_1 й S_2.

$$\begin{aligned} S_1&=r(\alpha)=e_1\beta_1+e_2\beta_2,\\ S_2&=r(\alpha)=e_1\beta_1^2+e_2\beta_2^2. \end{aligned} \tag{35}$$

Ці рівняння можна переписати в матричній формі таким способом:

$$\begin{bmatrix}\beta_1 & \beta_2\\ \beta_1^2 & \beta_2^2\end{bmatrix}\begin{bmatrix}e_1\\ e_2\end{bmatrix}=\begin{bmatrix}S_1\\ S_2\end{bmatrix}, \tag{36}$$

$$\begin{bmatrix}\alpha^3 & \alpha^4\\ \alpha^6 & \alpha^8\end{bmatrix}\begin{bmatrix}e_1\\ e_2\end{bmatrix}=\begin{bmatrix}\alpha^3\\ \alpha^5\end{bmatrix}. \tag{37}$$

Щоб знайти значення помилок e_1 і e_2, потрібно визначити зворотну матрицю для рівняння (37).

$$Inv\begin{bmatrix}\alpha^3 & \alpha^4\\ \alpha^6 & \alpha^1\end{bmatrix}=\frac{\begin{bmatrix}\alpha^1 & \alpha^4\\ \alpha^6 & \alpha^3\end{bmatrix}}{\alpha^3\alpha^1-\alpha^6\alpha^4}=\frac{\begin{bmatrix}\alpha^1 & \alpha^4\\ \alpha^6 & \alpha^3\end{bmatrix}}{\alpha^4-\alpha^3}=$$
$$=\alpha^{-6}\begin{bmatrix}\alpha^1 & \alpha^4\\ \alpha^6 & \alpha^3\end{bmatrix}=\alpha^1\begin{bmatrix}\alpha^1 & \alpha^4\\ \alpha^6 & \alpha^3\end{bmatrix}=\begin{bmatrix}\alpha^2 & \alpha^5\\ \alpha^7 & \alpha^4\end{bmatrix}=\begin{bmatrix}\alpha^2 & \alpha^5\\ \alpha^0 & \alpha^4\end{bmatrix}. \tag{38}$$

Тепер рівняння (37) ми можемо знайти з значення помилок.

$$\begin{bmatrix}e_1\\ e_2\end{bmatrix}=\begin{bmatrix}\alpha^2 & \alpha^5\\ \alpha^0 & \alpha^4\end{bmatrix}\begin{bmatrix}\alpha^3\\ \alpha^5\end{bmatrix}=\begin{bmatrix}\alpha^5+\alpha^{10}\\ \alpha^3+\alpha^9\end{bmatrix}=\begin{bmatrix}\alpha^5+\alpha^3\\ \alpha^3+\alpha^2\end{bmatrix}=\begin{bmatrix}\alpha^2\\ \alpha^5\end{bmatrix}. \tag{39}$$

З рівнянь (34) і (38) ми знаходимо поліном помилок.

$$e(X)=e_{j_1}X^{j_1}+e_{j_2}X^{j_2}=\alpha^2X^3+\alpha^5X^4. \tag{40}$$

Показаний алгоритм відновлює прийнятий поліном, видаючи в підсумку передбачуване передане кодове слово і, в остаточному підсумку, декодоване повідомлення.

$$U(X) = r(X) + e(X) = U(X) + e(X) + e(X),$$

$$r(X) = (100) + (001)X + (011)X^2 + (100)X^3 + (101)X^4 + (110)X^5 + (111)X^6,$$

$$e(X) = (000) + (000)X + (000)X^2 + (001)X^3 + (111)X^4 + (000)X^5 + (000)X^6,$$

$$U(X) = (100) + (001)X + (011)X^2 + (101)X^3 + (010)X^4 + (110)X^5 + (111)X^6 =$$

$$= \alpha^0 + \alpha^2 X + \alpha^4 X^2 + \alpha^0 X^3 + \alpha^6 X^4 + \alpha^3 X^5 + \alpha^5 X^6. \quad (41)$$

Оскільки символи повідомлення містяться у крайніх правих $k = 3$ символах, декодованим буде таке повідомлення:

$$\underbrace{010}_{\alpha^1}\underbrace{110}_{\alpha^3}\underbrace{111}_{\alpha^5}.$$

Це повідомлення в точності відповідає тому, що було обране для цього прикладу.

5. Висновки

Використовуючи отримані аналітичні залежності, у статті розроблена інформаційна технологія побудови системи OFDM-FHSS на основі оптимальних частотно-часових послідовностей та кодів Рида-Соломона.

Отримані результати можна використати на практиці для підвищення завадостійкості та зменшення складності реалізації засобів радіозв'язку, які використовують технологію OFDM-FHSS.

СПИСОК ЛІТЕРАТУРИ

1. Khan F. LTE for 4G Mobile Broadband. Air Interface Technologies and Performance / Khan F. – Cambridge: Cambridge University Press, 2009. – 509 p.
2. MIMO-OFDM Wireless Communications with Mathlab / Y. Cho, J. Kim, W. Yang [et al.]. – Singapore: John Wiley & Sons, 2010. – 457 p.
3. Ergen M. Mobile Broadband. Including Wimax and LTE / Ergen M. – Berkeley: Springer Science+Business Media, 2009. – 515 p.
4. Тузов Г.И. Статистическая теория приёма сложных сигналов / Тузов Г.И. – М.: Советское радио, 1977. – 400 с.
5. Варакин Л.Е. Системы связи с шумоподобными сигналами / Варакин Л.Е. – М.: Радио и связь, 1985. – 384 с.
6. Скляр Б. Цифровая связь. Теоретические основы и практическое применение / Скляр Б. – [2-е изд.]. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

Стаття надійшла до редакції 10.08.2012