

Данчул В.С.

студент,

Науковий керівник: Полторак В.П.

кандидат технічних наук, доцент,

Національний технічний університет України

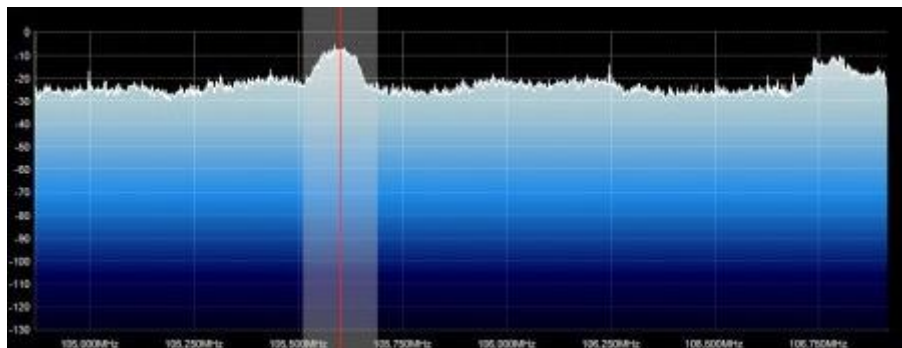
«Київський політехнічний інститут»

СПОСОБИ ПРИХОВУВАННЯ РАДІОСИГНАЛІВ

Передача даних є одним з основних моментів функціонування систем. Будь-яка система, що має у своєму складі більше одного елемента включає в себе певні канали зв'язку. Чим складніша система, тим більше каналів і тим вищі вимоги до них. Особливо важливим це є для систем керування. Необхідний захист від унеможливлення роботи системи шляхом постановки великої кількості завад. Особливо це стосується радіоканалів, середовище передачі яких не має природнього захисту.

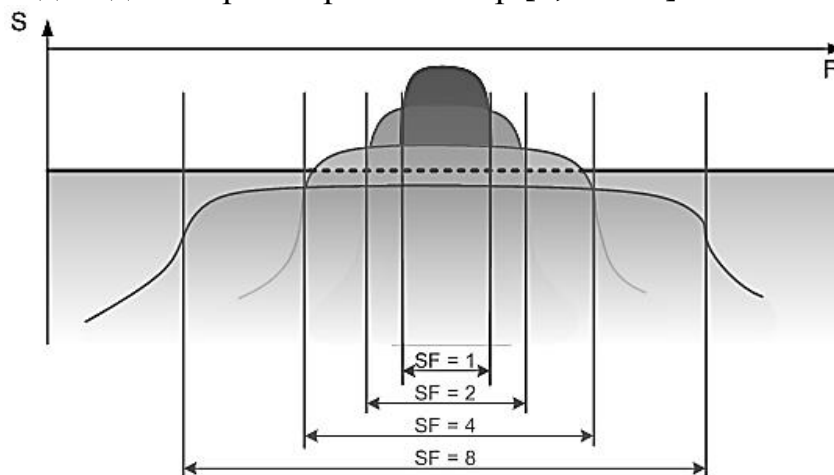
При високих вимогах щодо безпечності дуже доречним є використання «прихованої» передачі. Якщо передача не помітна то і доступ до даних отримати важче, оскільки спершу потрібно ще виявити передачу. Таким чином ми отримуємо додаткову надійність і можливість непомітної роботи системи, що у багатьох випадках є значною перевагою.

Якщо параметри сигналу не відомі, то єдиний спосіб його виявити – за енергією. Найбільш очевидним рішенням у такому випадку буде приховування сигналу шляхом обмеження його потужності такими чином, щоб приймач отримував повідомлення з гранично допустимою вірогідністю помилки. Чим далі приймач знаходиться від передавача, тим з меншою потужністю до нього доходить сигнал. Умовно середовище можна розділити на 3 зони – у першій сигнал приймається, у другій його можна помітити і у третій сигнал майже невиявний [2, с. 21]. Пошук сигналів відбувається шляхом аналізу спектру частотного діапазону.



Необхідно додати, що навіть якщо спектр сигналу зображено під рівнем шумів, це ще не означає що сигнал є непомітним. На його місці буде сума спектрів сигналу і шуму. Сторонній спостерігач може усереднювати спектральну щільність у часі. Обмеження потужності не єдиний спосіб приховування сигналу і, звичайно, не найбільш цікавий.

Потрібно відмітити, що потужність сигналу можна оцінити за площею його спектру. Якщо ми хочемо зберегти потужність і зменшити вірогідність виявлення, нам доведеться розширити спектр [1, с. 202].



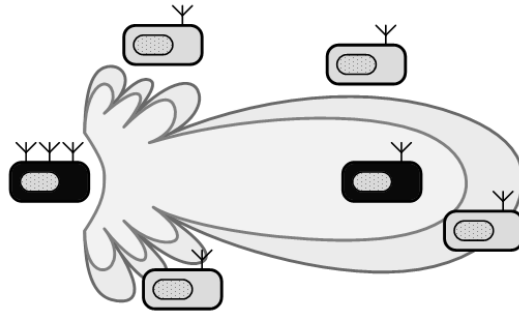
Існує декілька способів розширення. Можна рівномірно переміщувати сигнал по частотному діапазону, а при усередненні за часом ми побачимо широкий, рівномірний спектр. Цей метод називається FHSS (Frequency Hopping Spread Spectrum).

Початкова ширина спектру залежить від швидкості зміни сигналу (символів). Наприклад, якщо ми модулюємо фазу сигналу в залежності від інформаційного потоку, то чим швидше відбувається зміна фази, тим більшої широкосмуговості набуває сигнал. Звідси ми прийшли до іншого методу розширення – DSSS (Direct Sequence Spread Spectrum). При передачі кожний біт замінюється псевдовипадковою послідовністю. Псевдовипадковість потрібна для рівномірного розподілу потужності сигналу по діапазону частот.

Довжина послідовності прямо пропорційна коефіцієнту розширення спектра. В приймачі має застосовуватись корелятор, який буде розраховувати кореляцію прийнятого сигналу з опорною послідовністю і приймати рішення про переданий символ [1, с. 192]. Внаслідок застосування, відстань, на котру забезпечується якісний зв'язок зберігається, а область з високою вірогідністю детектування сигналу зменшується. DSSS застосовується в стандартах GPS, 802.11b, технології множинного доступу CDMA.

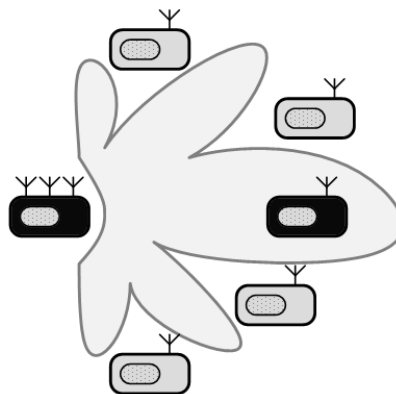
Окрім простого зменшення енергії, за допомогою DSSS можна ховати сигнал, наприклад, у спектрі телевізійного сигналу, а потім відновлювати за допомогою кореляційної обробки.

Іншим способом зменшення вірогідності виявлення сигналу є використання антенної решітки, тобто антени з набором випромінюючих елементів. Таким чином можна формувати діаграму направленості випромінювання, тобто випромінювати сигнал тільки в бік приймача [1, с. 202].



Перевага – економія енергії, недолік – потрібна пряма видимість між приймачем і передавачем, що є не завжди можливим.

Розглянемо також MU-MIMO технологію, що використовується в стандарті 802.11ac.



Кілька антенних елементів формують сигнал таким чином, щоб в зоні цільового приймача був максимальний рівень сигналу, а в зоні інших приймачів – мінімальний. За технологією MU-MIMO точка доступу формує такі паттерни для кожного користувача і передає їх суму одночасно, в одній полосі частот.

Позитивним моментом є те, що на відміну від попереднього рішення не вимагається пряма видимість між приймачем і передавачем.

Недоліки:

- місцезнаходження усіх приймачів повинне бути заздалегідь відоме (тобто необхідно знати паттерн кожного користувача);

- чим більша кількість учасників обміну, тим більша потрібна кількість антенних елементів.

Таким чином, останні дві розглянуті технології можна використовувати у системах зі статистичними елементами – збирати інформацію з датчиків, місцева сигналізація, тощо. Для рухомих об'єктів, наприклад, безпілотних літальних апаратів, пересувних роботів, вони непридатні. Найкращим рішенням в цьому випадку було б використання peer-to-peer CDMA. Ця технологія є перспективною для захищеного радіоуправління і існують патенти на її реалізацію, але готових рішень у відкритому розповсюдженні поки що немає.

Список використаних джерел:

1. Куприянов А. И., Сахаров А. В. Теоретические основы радиоэлектронной борьбы // Москва, 2007. – 356 с.
2. Мелихов С. В. Оценка чувствительность радиоприемных устройств: Учебно-методическое пособие // Томск: ТУСУР, 2012. – 100 с.