УДК 621.396

В. И. ВИШНЕВЕЦКИЙ, канд. техн. наук, *П. С. СМОРОДОВ*

ПОИСК СЛОЖНЫХ СИГНАЛОВ МЕТОДОМ РЕКУРРЕНТНОЙ ДЕШИФРАЦИИ

В системах передачи информации, использующих сложные сигналы, получаемые методом модуляции несущей бинарными псевдослучайными последовательностями (ПСП), предполагается решение задачи поиска и обнаружения сигналов с последующей оценкой их параметров, т. е. определение средней текущей частоты спектра принимаемых сигналов и изменяющегося запаздывания принимаемых сигналов относительно опорных псевдослучайных сигналов (ПСС).

Аппаратурная реализация теоретической возможности использования беспоисковых методов приема ПСС на основе построения многоканальных или согласованных фильтров с ростом длительности сигналов затруднительна, а при больших длительностях практически невозможна [1]. Поэтому исследование методов активного поиска ПСС и их оптимизация по времени поиска в системах передачи информации — актуальная задача.

Одним из корреляционных методов поиска ПСС длительности $N\tau=(2^n-1)\tau$ (1), где N — количество элементов в ПСП; n — разрядность генератора ПСП; τ — длительность единичного элемента ПСП, позволяющих уменьшить время поиска, является поиск методом последовательной оценки n двоичных символов [2]. Сущность последнего заключается в следующем: сначала оценивают (поэлементный прием) n последовательно принимаемых элементов ПСС, затем на интервале исследования T_e находят степень корреляции между опорным и принимаемым сигналами. При достаточных отношениях сигнал-шум (равных 1 ... 5 дБ) время поиска будет определяться в основном интервалом исследования T_e. Его выбирают достаточно большим, чтобы можно было пренебречь вероятностями ложной тревоги и пропуска сигнала, так как уменьшение интервала исследования T_e приводит к увеличению вероятностей ложной тревоги и пропуска сигнала. Последнее является причиной увеличения времени поиска. Однако это противоречие в значительной степени разрешается, если ПСС находить методом рекуррентной дешифрации, основанном на использовании структурных и рекуррентных свойств ПСС.

Метод рекуррентной дешифрации заключается в том, что после наблюдения любых $2n$ следующих друг за другом двоичных символов $a_{k-n}, a_{k-n+1}, \ldots, a_k, a_{k+1}, \ldots, a_{k+n-1}$ можно составить n неоднородных линейных рекуррентных уравнений (ЛРУ) с n неизвестными коэффициентами $h_1, \ldots, h_n$ [3]:

$$\begin{aligned} a_k &= h_1 a_{k-1} \oplus h_2 a_{k-2} \oplus \ldots \oplus h_n a_{k-n}; \\ a_{k+1} &= h_1 a_k \oplus h_2 a_{k-1} \oplus \ldots \oplus h_n a_{k-n+1}; \\ &\ldots\ldots\ldots\ldots \\ a_{k+n-1} &= h_1 a_{k+n-2} \oplus h_2 a_{k+n-3} \oplus \ldots \oplus h_n a_{k-1}, \end{aligned} \tag{2}$$

где символ $\oplus$ означает знак суммирования по модулю 2; h_i — коэффициенты полинома обратной связи,

$$h(x) = h_0 + h_1 x + h_2 x^2 + \ldots + h_n x^n. \tag{3}$$

Решив систему (2) в течение времени приема очередного $(2n+1)$-го элемента и сравнив полученные значения коэффициентов $h_1, h_2, \ldots h_n$ с заранее известными, при положительном результате сравнения можно однозначно определить положение принятого сегмента относительно всего периода ПСС и найти условное начало опорного ПСС. Оно согласовано с условным началом принимаемого ПСС.

Структурная схема устройства поиска ПСС, реализующего метод рекуррентной дешифрации, изображена на рис. 1. Двоичные символы a_i, принимаемого ПСС через открытый ключ k, поступают в $2n$-разрядный регистр и n-разрядный генератор ПСС (ГПСС). После приема $2n$ символов (в ГПСС будут записаны последние n символов из $2n$ принятых) они поступят в вычислительное устройство (ВУ), где строится и решается система ЛРУ (2). Если коэффициенты полинома обратной связи $h_i\,(i=1, \ldots, n)$, полученные в результате решения, совпадают с истинными коэффициентами, т. е. с комбинацией нулей и единиц, на которую настроен дешифратор (Дш), то он вырабатывает сигнал. По нему размыкается ключ k и запускается ГПСС. Последний начинает генерировать ПСС, синхронный с принимаемым.

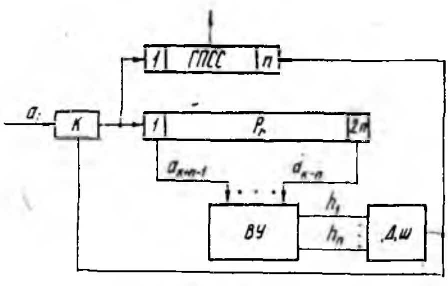

Рис. 1

Если результат решения ЛРУ не совпадает с истинными коэффициентами, то принимается следующий символ, содержимое регистра и ГПСС сдвигается на один разряд, строится и решается новая система ЛРУ, результат ее решения проверяется на соответствие истинным коэффициентам полинома обратной связи. И так до тех пор, пока не будет получено правильное решение.

Оценим помехоустойчивость такого метода поиска. Пусть p — вероятность правильного приема одного двоичного элемента ПСС. Тогда p^{2n} — вероятность правильного приема $2n$ элементов. Если $2n$ элементов приняты правильно, то после решения системы ЛРУ поиск прекращается, если нет, продолжается. Прием $2n$ элементов ПСС можно рассматривать как последовательность независимых испытаний, где вероятность успеха любого испытания равна p^{2n}. Поэтому количество испытаний до успеха k является случайной величиной, распределенной по геометрическому закону

$$P(k) = p^{2n}(1 - p^{2n})^{(k-1)}. \qquad (4)$$

Среднее число экспериментов до успеха $b = 1/p^{2n}$ (5). Количество экспериментов на одном периоде M-последовательности $l = 2^n - 1 - 2n + 1 = 2^n - 2n$ (6). Среднее время поиска $T_n = (t_р + 2n\tau)p^{2n}$ (7), где $t_р$ — время решения системы ЛРУ.

Необходимо, чтобы выполнилось условие $t_р \leqslant \tau$, т. е. решение системы ЛРУ следует получить за время приема следующего элемента ПСС. В противном случае количество экспериментов на одном периоде M-последовательности уменьшится.

Суммарная вероятность правильного обнаружения не позднее k-го эксперимента

$$P_\Sigma = \sum_{l=1}^{k} p^{2n}(1 - p^{2n})^{(l-1)} 1 - (1 - p^{2n})^k. \qquad (8)$$

При $k=l$ получим вероятность правильного обнаружения на одном периоде M-последовательности:

$$P_{\Sigma N} = 1 - (1 - (1 - p^{2^n})^{2^n - 2n)}. \qquad (9)$$

На рис. 2 показана зависимость вероятности правильного обнаружения на одном периоде M-последовательности $P_{\Sigma N}$ от вероятности правильного приема элемента p для значений $n=5$; 15 (сплошные кривые).

Сравним поиск ПСС методом рекуррентной дешифрации с поиском методом последовательной оценки n двоичных символов, реализованным в системе RASE [2]. При поиске методом последовательной оценки n двоичных символов суммарная вероятность правильного обнаружения не позднее x-го эксперимента [2]

$P_{\Sigma R} = 1 - (1 - p^n)^x$ (10). Количество экспериментов на одном периоде M-последовательности $l_R = |(2^n - 1)|/L$ (11),

где L — количество элементов M-последовательности, на которых проверяется наличие синхронизма; обозначение $\lfloor a \rfloor$ означает целую часть числа a.

Вероятность правильного обнаружения на одном периоде M-последовательности

$$P_{\Sigma R}^{(N)} = 1 - (1 - p^n)\, l_R. \qquad (12)$$

Зависимость $P_{\text{эр}}^{(N)}$ от p для $L=300$, $n=15$, что реализовано в системе RASE, показана на рис. 2 (пунктир).

Среднее время поиска $T_R = T_e / p^n$ **(13)**. Здесь T_e — время, в течение которого проверяется синхронизм, $T_e = L\tau$.

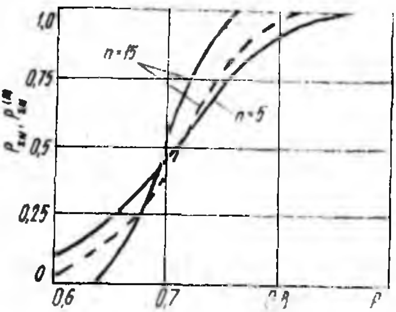

Рис. 2

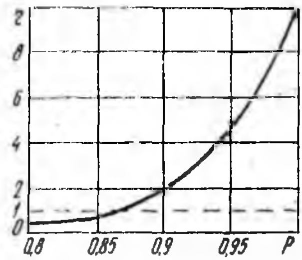

Рис. 3

Приравняв выражения (7), (13), найдем вероятность правильного приема, при которой время поиска для обеих систем будет одинаковым:

$$p_э = (t_р + 2n\tau)^{1/n}\, T_e. \text{ Пусть } t_р = \tau,\ L = mn, \text{ тогда}$$

$$p_э = \left(\frac{1+2n}{L}\right)^{1/n} \simeq \left(\frac{2n}{L}\right)^{1/n} = \left(\frac{2}{m}\right)^{1/n}. \qquad (14)$$

При $n=15$, $L=300$ из формулы (14) получаем $p_э = 0{,}86$. Этому значению при когерентном приеме ортогональных сигналов соответствует отношение сигнал-шум, равное 0,7 дБ. Если $p > 0{,}86$, то время поиска методом рекуррентной дешифрации будет меньше, чем в системе RASE.

Разделив выражение (13) на (7), определим выигрыш во времени поиска:

$$\eta = \frac{T_R}{T_n} = \frac{T_e p^{2n}}{p^n (t_p + 2n\tau)} = \frac{Lp^n}{1+2n} \simeq \frac{Lp^n}{2n} = 0{,}5\, m p^n. \qquad (15)$$

Предельное значение указанного выигрыша найдем при $p=1$: $\eta = 0{,}5\ m = 10$. Зависимость выигрыша во времени поиска от вероятности правильного приема элемента p показана на рис. 3.

Таким образом, при поиске ПСС методом рекуррентной дешифрации, когда $p > 0{,}675$, имеем более высокую вероятность правильного обнаружения на периоде M-последовательности (для $p > 0{,}675$), т. е. по сравнению с поиском методом последовательной оценки n двоичных символов данный метод является более помехоустойчивым (см. рис. 2). Кроме того, если $p > 0{,}86$, наблюдается выигрыш во времени поиска, и в случае увеличения вероятности правильного приема элемента он возрастает (рис. 3). Поэтому поиск ПСС методом рекуррентной дешифрации целесообразно применять при сравнительно больших отношениях сигнал-шум в полосе спектра *М*-последовательности.

Список литературы: 1. *Алексеев А. И.* Теория и применение псевдослучайных сигналов. М., 1969. 366 с. 2. *Уорд Р. Б.* Различение псевдослучайных сигналов методом последовательной оценки//Зарубеж. радиоэлектроника. 1966. № 8. С. 20—37. *3. Гай Бин Ю., Уорд Р. Б.* Метод дешифрации последовательности максимальной длины//Тр. Ин-та инж. по электротехнике и радиоэлектронике. 1977. Т. 65, № 7. С. 99—100.

Поступила в редколлегию 18.07.85