Захист інформації

УДК 621.391.1

И.Д. Горбенко, А.А. Замула, Е.А. Семенко

Харьковский национальный университет имени В.Н. Каразина, Харьков

УСКОРЕННЫЙ МЕТОД СИНТЕЗА ДИСКРЕТНЫХ СИГНАЛОВ С НЕОБХОДИМЫМИ СВОЙСТВАМИ ДЛЯ ПРИЛОЖЕНИЙ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ

Приведены результаты разработки метода синтеза дискретных криптографических сигналов с заданными свойствами. Проведен сравнительный анализ разработанного метода с известными методами с точки зрения производительности процедур поиска криптографических сигналов с необходимыми свойствами. Показано, что предлагаемый метод обладает значительным преимуществом в скорости отбора сигналов, отвечающих границам значений функций корреляции. Выигрыш достигается за счет применения метода «ветвей и границ», что сделало возможным исключить перебор всех вариантов сигналов для определения таких, которые отвечают необходимым условиям. Разработанные теоретические положения подтверждены средствами программного моделирования.

Ключевые слова: *сложные сигналы, корреляционная функция, помехозащищенность, скрытность, телекоммуникационная система, синтез, анализ, поле Галуа, метод.*

Введение

В настоящее время к основным показателям эффективности функционирования телекоммуникационных систем (и, в частности, мобильных сетей связи) относят [1]: пропускную способность, помехозащищенность, скрытность, безопасность, живучесть, своевременность доставки сообщений и др. [1]. Среди основных направлений улучшения данных показателей можно выделить направления, связанные с применением каналов с большой избыточностью, высокой пространственной, структурной, энергетической и временной скрытностью. Одним из путей решения данной проблемы является применение радиоканалов с частотной избыточностью (широкополосных каналов). Для ее обеспечения в настоящее время на физическом уровне используются фазоманипулированные широкополосные сигналы (ФМ ШПС) и частотно-фазоманипулированные (ЧФМ) сигналы. Однако построенные с их использованием каналы, не обеспечивают требуемые показатели по помехозащищенности и скрытности функционирования. Это в значительной степени связано с тем, что в качестве манипулирующих (расширяющих спектр) используются сигналы с линейным законом формирования. Такие сигналы обладают весьма ограниченными ансамблевыми характеристиками и низкой кодовой устойчивостью против раскрытия законов их формирования (низкой структурной скрытностью). Кроме того, повышение помехозащищенности, скрытности функционирования телекоммуникационных систем может быть достигнуто за счет изменения длительности (числа символов) ФМ ШПС или ЧФМ сигналов. Однако при использовании данных классов сигналов корреляционные, спектральные, ансамблевые и структурные свойства сигналов существенно ухудшаются, что, в свою очередь, приводит к ухудшению указанных выше характеристик функционирования телекоммуникационных систем [2 – 4].

Постановка проблемы. Как показали исследования [5 – 8] разрешение указанных противоречий и обеспечение требуемых показателей помехозащищенности, скрытности функционирования телекоммуникационной системы в условиях внутренних и внешних воздействий возможно на основе разработки методов анализа и синтеза нелинейных сложных криптографических сигналов с необходимыми корреляционными, ансамблевыми и структурными свойствами. В частности, при использовании таких сигналов в качестве физического переносчика информации временные затраты на раскрытие структуры используемых сигналов возрастают и постановка «оптимальных» помех становится проблематичной [7].

Анализ последних исследований и публикаций. В работах [8, 9] сформулирована и решена задача синтеза дискретных последовательностей, обеспечивающих требуемые значения помехозащищенности, информационной и структурной скрытности функционирования телекоммуникационной системы. Сложные сигналы, полученные на основе таких последовательностей (например, с применением системы расширения спектра методом прямой последовательности), обладают, с одной стороны, структурными свойствами, аналогичными свойствам случайных (псевдослучайных) последовательностей, а, с другой, - требуемыми ансамблевыми и

корреляционными свойствами. Кроме того, такие системы криптографических сигналов существуют и обладают указанными выше свойствами, для широкого спектра значений длин последовательностей.

Цель исследований. Для решения проблемы практического применения сигналов с нелинейными законами формирования в целях улучшения общесистемных показателей эффективности телекоммуникационных систем, необходимо разработать методы синтеза и анализа (исследования) систем дискретных сложных сигналов с необходимыми свойствами, способы и средства их формирования и обработки.

Изложение основного материала исследований

Отметим, что в целом ряде работ, посвященных синтезу и выбору дискретных последовательностей [3 – 6], приводятся верхние и нижние оценки распределения максимальных и минимальных лепестков функций авто- и взаимной корреляции. Нахождение дискретных последовательностей с необходимыми характеристиками корреляционных функций сводится, по сути, к перебору всех возможных последовательностей, принадлежащих некоторой системе сигналов, и отбору тех последовательностей, которые удовлетворяют известным оценкам. При этом вычислительная сложность таких методов весьма значительна. В данной работе приводятся теоремы, использование которых позволит существенно сократить время синтеза дискретных последовательностей, отвечающих необходимым требованиям с точки зрения значений боковых лепестков функции автокорреляции и обладающих улучшенными структурными свойствами. Задача выбора дискретных последовательностей, удовлетворяющих известным граничным оценкам, может быть записана в виде аналитических выражений:

$$Ra_1^1(l) \le \sum_{i=1}^{L} W_i^1 (W_{i+l}^1)^* \le Ra_2^1(l), l = \overline{0, L'}, \quad (1)$$

$$Ra_1^2(l) \le \sum_{i=1}^{L} W_i^2 (W_{i+l}^2)^* \le Ra_2^2(l), L' = \frac{L-1}{2},$$

если L - нечетное,

$$Ra_1^j(l) \le \sum_{i=1}^{L} W_i^j (W_{i+l}^j)^* \le Ra_2^j(l), L' = \frac{L}{2},$$

если L - четное,

$$\vdots$$

$$Ra_1^N(l) \le \sum_{i=1}^{L} W_i^N (W_{i+l}^N)^* \le Ra_2^N(l),$$

где $Ra_1^i(e), Ra_2^i(e)$ – граничные значения боковых лепестков ФАК, L – период последовательности W_i^{υ}, $\upsilon = \overline{1, N}$.

Теорема 1. Пусть максимальные (минимальные) значения реализаций функций $Ra_1^1(l)$ и $Ra_2^1(l)$ в (1) являются таковыми, что величина δ, определенная как

$$\delta = \left|Ra_1'(l) - Ra_1(l)\right| \text{ либо } \delta = \left|Ra_2'(l) - Ra_2(l)\right|, \quad (2)$$
$$\delta \ne 0,1,2,...P-1,P,$$

больше P, а W^j - сигнал определен над полем GF(P) или над кольцом чисел по модулю P, тогда множество значений циклической свертки (функции автокорреляции (ФАК)) $Ra^Z(l)$ может принадлежать интервалу

$$(\min Ra_1(l), \max Ra_2(l)), \quad (3)$$

по крайней мере при "отбрасывании" r последних и "добавлении" r первых символов сигнала W, где

$$r = \frac{\delta}{P}, \text{ если } \delta \,|\, P \text{ и } r = \frac{\delta + t}{P}, \text{ если } \delta \ne P.$$

Доказательство теоремы 1.

Предположив, что $Wa_1'(l) < \min Ra_1(l)$, рассмотрим ФАК сигнала. Так как символы W^j определены в кольце чисел по модулю P, либо над полем GF(P), то при «отбрасывании» W_1 и «добавлении» W_{L+1}, Ra_1' возрастает по крайней мере на P. Аналогично при «отбрасывании» символа W_2 и «добавлении» W_{L+2}, Ra_1' возрастает не более чем на P. И, таким образом, после r «отбрасываний» $\min Ra_1'(l)$ и добавлений r символов каждый с максимальным расстоянием P

$$\min Ra'(l) \ge Ra_1'(l) + P \cdot r, \quad (4)$$

поэтому

$$r' \ge \frac{\min Ra'(l) - Ra_1'(l)}{P}. \quad (5)$$

В действительности величина $r > r'$, а вероятность того, что за r шагов $Ra'(l)$ станет равной значению $\min Ra'(l)$ и достаточно мала.

Рассмотрим второй случай, когда

$$Ra_2'(l) > \max Ra_2(l).$$

Рассуждая аналогично вышеприведенному, после r шагов получим

$$\max Ra_2(l) < \max (Ra_2'(l) - P \cdot r)$$

и

$$r \ge \frac{\max Ra_2'(l) - Ra_2(l)}{P} \quad (6)$$

С учетом (4) и (6), дополняя их величиной t, но так, чтобы $(\delta + t)$ являлось делителем P, имеем

$$r = \frac{\delta}{P}, \text{ если } \delta | P \text{ и } r = \frac{|\delta| + t}{P}, \text{ если } \delta \text{ не делит } P.$$

Следствие теоремы 1. Если $W_i \in GF(P)$, то $r = \frac{\delta}{2}$, если δ – четное и $r = \frac{\delta + 1}{2}$, если δ нечетное.

Подчеркнем, что теорема 1 и ее следствие имеют важное значение, так как из них следует, что за $r < r'$ «отбрасываний» и r «дополнений» $\min Ra'(l)$, и $\max Ra_2'(l)$ не может попасть в интервал $(\min Ra_1(l), \max Ra_2(l))$.

Теорема 2. Пусть подпространство $\left\{W^j\right\}$ есть множество сигналов длительности L над полем $GF(P)$, тогда необходимым условием n-уровневости по циклической автосвертке с уровнями K_i каждого из W^j является условие не более чем γ - неуравновешенности (несбалансированности) в числе символов (1) K^1 и (-1) K^{-1}, причем

$$\gamma = \left|K^1 - K^{-1}\right| \le \sqrt{L + \sum_{i+1}^{n} n_i R_i} \qquad (7)$$

Доказательство теоремы 2.

Из анализа свойств бинарных сигналов, приведенных в [8, 9], вытекают необходимые условия существования множества сигналов W^j с n-уровневой автосверткой (ПФАК), которые можно представить в виде системы уравнений

$$\sum_{i=1}^{n} n_i = L - 1; \qquad \sum_{i=1}^{n} n_i k_i^{+} = k^1(k^1 - 1);$$

$$R_1 = L - 4(k^1 - k_1^{+}); \qquad (8)$$

$$R_2 = L - 4(k^1 - k_2^{+}); \ldots R_n = L - 4(k^1 - k_n^{+}),$$

где k_i^{+} – число произведений вида (1) $\cdot$ (-1).

Определим значения k_i^{+} из n последних уравнений системы (8) и подставим их во второе уравнение. В результате получим

$$\sum_{i=1}^{n} \frac{R_i - L + 4k^1}{4} = \frac{1}{4}\sum_{i=1}^{n} n_i R_i - \frac{L}{4}\sum_{i=1}^{n} n_i + k^1 \sum_{i=1}^{n} n_i = \qquad (9)$$

$$= k^1\left(k^1 - 1\right).$$

Упростив выражение (9) с учетом первого уравнения системы (8), получим

$$(k^1)^2 = k^1 L + \frac{1}{4}\left[(L-1) / L - \sum_{i=1}^{n} n_i R_i\right] = 0, \qquad (10)$$

а решая уравнение (10) относительно k^1, получим

$$k^1 = \frac{L}{2} \pm \sqrt{L + \sum_{i+1}^{n} n_i R_i}. \qquad (11)$$

Учитывая, что общее количество символов (+1) и (-1) равно L, а также то, что при выборе w^j $R_j \le \max R_i$, $i, j = \overline{1,n}$, получим необходимые условия существования двоичного сигнала с n-уровневой ПФАК:

$$\frac{L}{2} - \sqrt{L + \sum_{i=1}^{n} n_i R_i} \le k^1 \le \frac{L}{2} + \sqrt{L + \sum_{i=1}^{n} n_i R_i};$$

$$\frac{L}{2} - \sqrt{L + \sum_{i=1}^{n} n_i R_i} \le k^{-1} \le \frac{L}{2} + \sqrt{L + \sum_{i=1}^{n} n_i R_i}; \qquad (12)$$

$$k^{+1} + k^{-1} = L.$$

Из выражения (12) следует, что необходимым условием существования двоичных векторов с n - уровневой ПФАК является ограничение на неуравновешенность в числе символов (1) и (-1):

$$\gamma = \left|k^1 - k^{-1}\right| \le \sqrt{L + \sum_{i=1}^{n} n_i R_i}. \qquad (13)$$

Теорема 3. Пусть W^j – вектор, символы которого при временном представлении принимают значения над полем $GF(P)$, а неуравновешенности в числе символов, определенные относительно величины r как $\delta_i = \left|k - r\right|$ – соответственно $\delta_1, \delta_2, \ldots, \delta_r$ тогда вектор W^j, удовлетворяющий необходимым условиям, может быть образован только посредством отбрасывания и добавления, по крайней мере

$$G = \frac{1}{r}\sum_{i=1}^{r} \delta_i \quad \text{символов.} \qquad (14)$$

Доказательство теоремы 3.

Предположим, мы отбрасываем символы $W_1^j, W_2^j, \ldots, W_q^j$, по которым существует асимметрия относительно величины r, а добавляем символы $W_{L+1}^j, W_{L+2}^j, \ldots, W_{L-k}^j$, тогда асимметрия может быть устранена, по крайней мере, только через $G = \frac{1}{2}(\delta_1 + \delta_2 + \ldots + \delta_k)$ шагов. Коэффициент $1/2$ выбран из условия, что все добавляемые символы уменьшают асимметрию.

В действительности, вследствие псевдослучайности символов над полем $GF(P)$ значение числа шагов может быть определено как

$$G^{+} = GZ,$$

где $Z \ge 1$ коэффициент, выбираемый в зависимости от статистических свойств источника символов сигнала.

В ходе исследований было проведено имитационное моделирование собственно синтеза последовательностей, основанного на приведенных выше теоремах, и производительности (быстродействия) такого метода. В качестве источника дискретных последовательностей были использованы последовательности, получаемые на выходе схемы разворачивания ключа криптографического алгоритма – стандарта шифрования США AES [10]. В качестве ключевой последовательности был использован сегмент размерностью 10000 символов. В процессе моделирования с помощью метода «прибавлений и «добавлений» были выбраны последовательности символов, отвечающие границе «плотной упаковки» для указанного периода последовательности. Анализ показал (было проведено 1000 испытаний), что данный метод обеспечивает выигрыш в производительности синтеза дискретных последовательностей более 45 процентов по сравнению с методом перебора всех возможных вариантов последовательностей для указанного пе-

риода. При реализации рассматриваемого метода возможны пропуски (потери) в нахождении лучших сигналов. Но как показали исследования, процент таких потерь – незначителен, и для указанного периода составляет не более 8 процента.

Выводы

Наличие боковых пиков у функции неопределенности (ФН) сложных сигналов приводит к увеличению неоднозначности при различении сигналов, и к увеличению времени вхождения в синхронизм. Применение линейных правил построения манипулирующих (адресных) дискретных последовательностей, не позволяет обеспечить требуемые, для целого ряда приложений телекоммуникационных систем, скрытность функционирования. При выборе или синтезе сложных сигналов в процессе построения телекоммуникационной системы необходимо использовать сигналы с малыми боковыми пиками ФН (сигналы с хорошими корреляционными свойствами), а также с нелинейными законами их формирования.

Разработаны основные теоретические положения оптимизации с помощью метода ветвей и границ выбора сигналов с необходимыми свойствами. Применение таких сложных криптографических сигналов позволит повысить помехозащищенность, скрытность функционирования телекоммуникационной системы, осуществить кодовое разделение абонентов в многопользовательских системах связи, в частности CDMA.

В качестве перспективных исследований в этом направлении следует выделить получение количественных показателей помехозащищенности, скрытности функционирования телекоммуникационных систем, достигаемых на основе применения нелинейных классов сигналов в условиях различных внешних и внутренних воздействий на систему.

Список литературы

1. Воробієнко П.П. Телекомунікаційні та інформаційні мережі: Підручник / П.П. Воробієнко, Л.А. Нікітюк, П.І. Резніченкко. – К: САММІЕ – Книга, 2010. – 708 с.

2. Варакин Л.Е. Системы связи с шумападобными сигналами / Л.Е. Варакин. – М.: Связь, 1985. – 384 с.

3. Ipatov V.P. Spread Spectrum and CDMA.Principles and Applications [Текст] / V.P. Ipatov. – University of Turku, Finland and St. Petersburg Electrotechnical University 'LETI', Russia. - John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England. - 2005. – 385 p.

4. Свердлик М. Б. Оптимальные дискретные сигналы / М.Б. Свердлик. – М: Радио и связь, 1975. – 200 с.

5. Sarvate D.V. Crosleration Properties of Pseudorandom and Related Sequences / D.V. Sarvate, M.V. Pursley // IEEE Trans. Commun. Vol. Com 68-5, 1980.

6. Замула А.А. Мощность метода кодирования характеристических дискретних сигналов / А.А. Замула // Системи обробки інформації: – Х.: ХУПС, 2014. – Вип. 2 (118) – С. 162 – 168.

7. Замула А.А. Предложения по построению широкополосных систем передачи со сложными сигналами / А.А. Замула // Радиотехника. – Х. ХНУРЕ, 2012 – Вып. 4, № 171. – С. 177-185.

8. Метод синтеза сигналов с заданными ограничениями на уровень боковых лепестков корреляционной функции / А.А. Замула, Р.И. Киянчук, Т.Е. Ярыгина, Е.П. Колованова // Восточно-европейский журнал передових технологий. – 2011. – № 5/9 (53). – С. 30 – 34.

9. Горбенко И.Д. Синтез систем сложных сигналов с заданными свойствами корреляционных функций для приложений многопользовательских систем с кодовым разделением абонентов / И.Д. Горбенко, А.А. Замула, Е.А. Семенко // Системи обробки інформації. – Х.: ХУПС, 2014. – Вип. 9 (125). – С. 25 – 30.

10. Горбенко І.Д. Прикладна криптологія: Теорія. Практика. Застосування: Монографія. / І.Д. Горбенко, Ю.І. Горбенко. – Х.: Форт, 2012. – 880 с.

Поступила в редколлегию 15.12.2014

Рецензент: д-р техн. наук, проф. В.А. Краснобаев, Полтавский национальный технический университет имени Юрия Кондратюка, Полтава.

ПРИСКОРЕНИЙ МЕТОД СИНТЕЗУ ДИСКРЕТНИХ СИГНАЛІВ З НЕОБХІДНИМИ ВЛАСТИВОСТЯМИ ДЛЯ ДОДАТКІВ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ І МЕРЕЖ

І.Д. Горбенко, О.А. Замула, Є.О. Семенко

Наведені результати розробки метода синтеза дискретних сигналів з необхідними властивостями. Проведений порівняльний аналіз розробленого метода з відомими методами з точки зору швидкодії процедур пошуку сигналів з необхідними властивостями. Показано, що метод, який пропонується, має значні переваги у швидкості відбору сигналів, що задовольняють границям значень функції кореляції. Виграш досягається за рахунок операцій, що не визначають необхідності перебору усіх можливих варіантів сигналів для визначення таких, що відповідають необхідним умовам. Розроблені теоретичні положення підтверджені засобами програмного моделювання.

Ключові слова: *складені сигнали, кореляційна функція, завадо захищеність, скритність, телекомунікаційна система, синтез, аналіз, поле Галуа, метод.*

SHORTCUT METHOD OF DISCRETE SIGNAL SYNTHESIS WITH REQUIRED PROPERTIES FOR TELECOMMUNICATION SYSTEM AND NETWORK APPLICATIONS

I.D. Gorbenko, A.A. Zamula, E.O. Semenko

The article contains results of method elaboration of discrete signals with given properties synthesis. Comparative study of elaborated method with known methods from the viewpoint of the output of signals with required properties search procedures was conducted. It is shown that the suggested method possesses a considerable advantage in speed of signal takeout corresponding to ranges of correlation function values. The gain is reached due to operations that do not presuppose the necessity of searching all possible signal variants for determining those corresponding to required conditions.

Keywords: *analysis, complex signals, correction function, Galois field, method, noise immunity, secrecy, synthesis, telecommunication system.*