ЗАЩИТА РЕСУРСОВ ИНФОРМАЦИОННЫХ СИСТЕМ НА ОСНОВЕ СЛОЖНЫХ СИГНАЛОВ

Горбенко И.Д., Замула А.А.
Харьковский национальний университет радиоэлектроники
61166, Харьков, проспект Ленина 14, кафедра безопасности информационных технологий, тел. (057)7021425, E – mail: alexz_@bk.ru

The report suggests methods for the synthesis of a class of complex signals based on the properties of Galois fields. In addition, a theorem on which the characters are established connection elements of the multiplicative group of the Galois field and the dependence of the characters of discrete codes, which use the characters of the multiplicative group. The proposed work describes the ensemble, correlation, statistical and structural properties of one type of complex signals. The possibility of improving immunity, secrecy of the system transfer information using this class of signals.

Введение

Системы передачи информации являются одним из основных видов радиотехнических систем и быстро развиваются во многих отношениях. К таким системам предъявляются все более жесткие требования по обеспечению их работы в условиях сложных внешних воздействий, а так же естественных и преднамеренных помех и помех от других радиотехнических систем, работающих на близких частотах или в общем участке диапазона частот.

Важными характеристиками некоторых систем передачи информации являются помехоустойчивость и скрытность функционирования. Под помехоустойчивостью понимают способность системы противостоять воздействию мощных помех. Скрытность функционирования системы предполагает способность системы функционировать в режиме, затрудняющим обнаружение передаваемых сообщений и оценку их параметров специальной разведывательной аппаратурой злоумышленника. Одним из видов скрытности является информационная скрытность. Такой вид скрытности предполагает целый комплекс мер, методов и средств для затруднения определения злоумышленником: самого факта передачи сообщений по каналам связи, содержания передаваемых сообщений и другое. Комплексное решение проблемы обеспечения помехоустойчивости, скрытности функционирования системы передачи информации может быть достигнуто, в том числе, на основе реализации динамического режима передачи информации, при котором соответствие: бит сообщения – сигнал меняется с течением времени по закону, предсказание которого возможно с вероятностью, не превышающей допустимую. Одним из путей достижения заданной помехоустойчивости, является реализация частотной избыточности в канале связи.

Большое значение при решении задач обеспечения требуемой помехоустойчивости и скрытности функционирования (в том числе, информационной скрытности) имеют исследования, связанные с использованием новых видов сигналов, получивших название: сложных, широкополосных, многомерных и шумоподобных. Разработка методов синтеза сложных сигналов с хорошими корреляционными, ансамблевыми, статистическими, структурными и другими свойствами является актуальной задачей.

При радиоэлектронном противодействии эффективная помеха может быть организована только после обнаружения присутствия противостоящей системы в эфире и оценки таких ее параметров как частотный диапазон и занимаемая полоса. Если скрытная система использует сигнал с некоторым законом модуляции, параметры которого неизвестны перехватчику, то последний лишен возможности применения согласованного фильтра или коррелятора для обнаружения сигнала. В этих условиях у противостоящей системы нет иного выбора, как рассматривать перехватываемый сигнал в виде случайного и основывать его обнаружение только на факте появления или отсутствия некоторого избытка энергии в некотором участке частотного диапазона. Перехватчик применяет энергетический детектор, называемый также радиометром, который является оптимальным с точки

зрения обнаружения ограниченного по полосе шумового сигнала на фоне аддитивного белого гауссовского шума [1].

Перехватчику могут быть неизвестны заранее сведения о частотном диапазоне и интервале времени, занимаемом сигналом. Учитывая эти обстоятельства, его стратегия будет заключаться в комбинировании указанных параметров, осуществляя процедуру обнаружения либо путем сканирования частотно-временной области, либо используя набор параллельных каналов, каждый из которых ответственен за анализ ограниченного участка частотно-временной области. В любом случае качество работы приемника системы-перехватчика будет полностью определяться характеристикой энергетического детектора, настроенного на истинную для перехватываемого сигнала частотно-временную зону. В свою очередь, у скрытной системы имеется только единственная возможность предотвратить обнаружение своего сигнала потенциальным перехватчиком: использовать сигналы с распределенным спектром, обладающие максимально возможным значением выигрыша от обработки (произведение полосы частот, занимаемой сигналом на его длительность). Единственной причиной, вынуждающей перехватчик прибегнуть к такому неэффективному инструменту как энергетический приемник, является отсутствие информации о структуре обнаруживаемого сигнала, т.е. его закона модуляции. По этой причине перехватчик не может обрабатывать сигнал аналогично приемнику скрытной системы (т.е. осуществлять согласованную фильтрацию). Очевидно, что в случае недостаточной структурной сложности сигнала и осведомленности перехватчика о его возможных альтернативных вариантах, последний может попытаться их все реализовать. Соответствующим оборудованием для этого может служить набор параллельных согласованных фильтров либо единый перестраиваемый фильтр (несколько фильтров), пригодный для обработки сигналов различных по структуре последовательно во времени, если сигнал, который необходимо обнаружить, принимается достаточно долго. Поэтому другая сторона стратегии скрытной системы в борьбе с перехватчиком состоит в применении сигналов с практически не раскрываемой структурой.

Основное содержание исследований

В приложениях, имеющих дело с безопасностью информации, степень защиты данных определяется числом равновероятных ключей, с помощью которых криптоаналитик старается взломать шифротекст, т.е. зашифрованные данные. Применительно к структуре сигнала каждый из таких ключей есть ничто иное, как закон модуляции, который, как правило, повторяется с периодом T. Предположим, что сигнал построен на основе M - ичного алфавита, т.е. возможны M реализаций индивидуального сигнального элемента (чипа). Если полоса, отводимая системе, равна W, то общее сигнальное пространство имеет размерность, определяемое как WT, т.е. закон модуляции может быть сконструирован посредством WT чипов. Очевидно, что величина M^{WT} определяет общее число различных законов модуляции, т.е. число ключей, и, значит, разработчик, отвечающий за секретность модуляционного формата разрабатываемой системы, должен использовать сигналы с достаточно большим выигрышем от обработки. Таким образом технология широкополосности в значительной степени способствует криптографической защите структуры сигнала.

Усилия исследователей направлены на поиски ансамблей сложных сигналов, характеристики которых с ростом длины приближаются к характеристикам гипотетического ансамбля, т.е. ансамбля, все представители которого обладают нулевой постоянной составляющей, идеальной периодической автокорреляционной функцией (ПФАК) и нулевой периодической функцией взаимной корреляции (ПФВК). Широко распространенным критерием подобного приближения является минимаксный критерий, ориентирующий синтез ансамбля на минимизацию максимального значения на множестве всех нежелательных корреляций. Для идеального гипотетического ансамбля корреляционный пик как наибольшее из двух величин: максимума среди всех боковых лепестков автокорреляций последовательностей и максимума среди значений взаимных корреляций всех пар

последовательностей равны нулю, а для любого реального ансамбля корреляционный пик может служить адекватной мерой его близости к идеальному.

Ансамбли со значением корреляционного пика достигающие предела, предсказываемого нижними границами Велча и Сидельникова [1], являются оптимальными по критерию корреляционного пика, и иногда называются минимаксными.

Синтез семейств сигналов с необходимыми авто и взаимно корреляционными свойствами заключается в отыскании семейства дискретных последовательностей, обладающего соответствующими авто и взаимно корреляционными функциями. Искусство проектирования широкополосных систем во многих аспектах базируется на нахождении сигналов с соответствующими корреляционными свойствами.

Минимизация уровня боковых лепестков автокорреляционной функции (АКФ) имеет наибольшее значение при конструировании сигнала для таких приложений как измерение времени запаздывания, временное разрешение и др. Следует иметь в виду, что равенство нулю всех боковых лепестков невозможно для финитных или апериодических фозоманипулированных сигналов.

При синтезе сигналов применяют минимаксный критерий, который требует достижения минимально возможной величины максимального бокового лепестка АКФ апериодического кода. Очевидно, что предпочтительными являются кодовые последовательности с наименьшим значением максимального бокового лепестка. Таким образом требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка АФАК.

Сформулированная выше оптимизационная задача, как и многие другие задачи дискретной оптимизации, не имеют общего аналитического решения.

Обсуждаются методы синтеза оптимальных бинарных последовательностей большой длины с заданными авто - и взаимнокорреляционными свойствами.

Рассмотрены так называемые характеристические дискретные сигналы (ХДС) с числом позиций (символов) $L = 4x + 2$ и $L = 4x$, синтез которых базируется на использовании характера ψ мультипликативной группы поля $GF\,(P)$ [2].

Правило кодирования таких кодов, например, для $L = 4x + 2$ имеет вид [2]:

$$\mu = \{\mu_i : i = 0, 1, \ldots, P-2\}$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\mathrm{mod}\, P),$$

$$\mu_i = 1, \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\, P), \qquad (1)$$

$$\mu_i = \psi(\Theta^i + 1), \text{ если } \Theta^i + 1 \not\equiv 0 (\mathrm{mod}\, P),$$

$$\mu_i = -1, \text{ если } \Theta^i + 1 \equiv 0 (\mathrm{mod}\, P), \qquad (2)$$

где Θ - первообразный элемент поля $GF\,(P)$.

Мощность метода кодирования данного класса сигналов (М) равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы на смежные классы по классу автоморфных коэффициентов, и определяется как $M = \varphi(L)/2$.

Известно так же [2], что правила кодирования ХДС с числом позиций (символов) $L = 4x + 2$ приводят к коду с двухуровневой периодической функцией автокорреляции $R_\mu = \{-2, 2\}$.

Максимальные по модулю значения боковых лепестков функции автокорреляции импульсного бинарного фазоманипулированного сигнала, построенного на базе кода μ находятся в пределах $(0{,}47 \div 0{,}82)/\sqrt{L}$.

Способ формирования ХДС длительностью L, который приведен в работе [2], сводится к составлению таблицы соответствия i-й элемент поля ($a_i = \theta_j^i + 1$ (θ_j^i - первообразный элемент поля)) - i-й индекс. Для составления таблицы необходимо решить L сравнений вида:

$$a_i \equiv \Theta_j^{U_i} (\mathrm{mod}\ P),\ i = \overline{0, P-1}, \qquad (3)$$

где Ui – индекс элемента поля GF(P), определяемый из решения сравнения (1). Данный способ из-за отсутствия алгоритмизируемых процедур трудно осуществим.

В работах [3,4] предложены способ и устройство формирования ХДС. Способ основан на рекуррентной зависимости между элементами и индексами элементов поля Галуа, при этом становится возможным алгоритмизировать процедуры формирования символов ХДС. Однако вычислительная сложность, (время формирования ХДС) остается значительной.

Приводятся теоремы, на основании которых устанавливаются связи характеров элементов мультипликативной группы поля Галуа и зависимость символов дискретных кодов, построенных на использовании характеров мультипликативной группы поля. Выявленные и описанные в теоремах связи элементов и характеров элементов поля позволяют алгоритмизировать процедуры формирования символов ХДС, и, кроме того, повысить быстродействие устройств формирования ХДС что несомненно оказывает влияние на успешное решение ряда задач, в том числе, реализацию динамического режима передачи информации.

Формулируется и приводится доказательство теоремы, с использованием которой появляется возможность синтезировать все множество изоморфизмов характеристических дискретных сигналов. Показано, такой синтез может быть реализован посредством децимации сигнала, построенного по одному из первообразных элементов поля Галуа. Формулируются требования к выбору коэффициентов децимации.

Даются оценки помехоустойчивости и скрытности функционирования системы передачи информации при использовании характеристических дискретных сигналов.

Выводы

В докладе приводится анализ возможностей применения различных ансамблей минимаксных последовательностей для ряда приложений информационных систем, в частности, в качестве: манипулирующих или расширяющих спектр в системах передачи информации с шумоподобными сигналами, управляющих последовательностей в системах передачи информации с псевдослучайной перестройкой рабочей частоты, «исходного материала» для ключевых последовательностей символов в криптографии и др.

Литература:

1. Valery P. Ipatov Spread Spectrum and CDMA principles and Applications// Univesity of Turku.

2. Свердлик М.Б. Оптимальные дискретные сигналы. М., 1975. 200 с.

3. Горбенко И.Д., Замула А.А.. Ускоренные алгоритмы построения систем характеристических дискретных сигналов //Радиотехника. 1988. Вып. 84. с.69-72.

4. А.с. СССР Устройство для формирования псевдослучайных сигналов / В.И. Долгов, И.Д. Горбенко – 1983.- № 5. – с. 63.