Keywords: *optical fiber, optical cable, modular tube, excess fiber length, curvature, bend radius climatic test.*

Бурдин Владимир Александрович, проректор по науке и инновациям, д.т.н., профессор Кафедры линий связи и измерений в технике связи (ЛС и ИТС) Поволжского государственного университета телекоммуникаций и информатики (ПГУТИ). Тел. (8-846) 332-21-61; E-mail: burdin-va@psuti.ru

Важдаев Михаил Александрович, аспирант Кафедры ЛС и ИТС ПГУТИ. Тел. 8-917-817-64-51; E-mail: rip86rs@mail.ru

УДК 621.393

ОБОБЩЕННЫЙ ИНВАРИАНТНЫЙ МЕТОД ПЕРЕДАЧИ СООБЩЕНИЙ И ОЦЕНКА ЕГО ИНФОРМАЦИОННОЙ ЗАЩИЩЕННОСТИ

Лебедянцев В.В.

В работе синтезирован обобщенный инвариант линейных каналов связи в виде сохраняемого каналами отношения объемов *m*-мерных параллелепипедов, образуемых в сигнальном пространстве соответствующими группами передаваемых сигналов. Разработан алгоритм передачи сообщений, использующий данный инвариант. Дана оценка информационной защищенности обобщенного инвариантного метода передачи сообщений.

Ключевые слова: группа преобразований, инвариант, обобщенный инвариантный метод передачи, информационная защищенность.

Введение

Так называемые системы связи с инвариантными характеристиками помехоустойчивости в систематизированном виде впервые были описаны в [1]. В этой работе рассматривалась проблема обеспечения инвариантности (нечувствительности) систем связи к воздействию аддитивных и неаддитивных помех, введены понятия абсолютной и относительной инвариантности. Относительная инвариантность означает, что при наличии в канале флуктуационной помехи вероятность ошибки при воздействии основной помехи не превышает определенной, обусловленной влиянием флуктуационной помехи, величины.

Для обеспечения инвариантности к аддитивным помехам предложено несколько способов, базирующихся либо на выборе сигнала, либо на выборе демодулятора, а также на применении адаптивных методов приема. Инвариантность к неаддитивной (мультипликативной) помехе обеспечивалась применением соответствующего метода модуляции.

Более общий подход к решению проблемы инвариантной относительно свойств канала передачи сообщений предложен в [2], а промежуточные итоги исследований приведены в [3]. Этот подход базируется на представлении преобразований сигналов в канале связи элементами аппаратуры, средой распространения и разнообразными помехами соответствующими группами преобразований. Группы преобразований обладают набором инвариантов – некоторыми соотношениями между параметрами сигналов, остающимися неизменными при изменениях самих сигналов. В силу этого свойства инварианты являются идеальной формой представления элементов сообщений для их безыскаженной передачи по каналу связи. Разумеется, при наличии в канале флуктуационной помехи можно обеспечить лишь относительную инвариантность.

Как показано в [3], преобразование сигналов элементами аппаратуры и средой распространения линейного канала связи описывается аффинной группой преобразований с одним из инвариантов в виде отношения длин векторов сигналов, имеющих одинаковое направление (в геометрической интерпретации – отношения длин отрезков, лежащих на одной прямой).

Влияние аддитивных помех описывается группой преобразований типа сдвигов векторов сигналов в направлении векторов помехи. У этой группы преобразований инвариантом является расстояние в сигнальном пространстве, измеряемое вдоль прямой, перпендикулярной направлению векторов помехи. Сочетая инварианты аффинной группы преобразований и группы сдвигов, можно получить инвариантную амплитудную модуляцию для линейных каналов с аддитивными помехами [3]. Преимуществом нового способа описания каналов связи является наличие в теории групп преобразований универсального метода синтеза инвариантов для любой группы. Для этого используются так называемые инфинитезимальные операторы [4]. Это обстоятельство существенно облегчает синтез инвариантных систем связи.

Дальнейшее развитие теории инвариантных систем связи предполагает поиск новых более общих инвариантов каналов связи, синтез соответствующих инвариантных методов модуляции и оценку их информационной защищенности.

Синтез обобщенного инварианта для линейных каналов связи

Синтезированный в [3] инвариант линейного канала в форме отношения длин векторов сигналов подобной формы предполагает использование сигналов, концы векторов которых лежат на прямой, проходящей через начало координат сигнального пространства. Это ограничивает разнообразие применяемых сигналов и, соответственно, информационную защищенность, помехоустойчивость и другие качественные характеристики системы связи. Поэтому целесообразным является нахождение инварианта линейного канала, не накладывающего жесткие ограничения на форму передаваемых сигналов.

Выберем для отображения вектора сигнала $\bar{s}_{вых}$ на выходе канала некоторую систему координат $\bar{y}_1, \bar{y}_2, ..., \bar{y}_n$. Как показано в [3], множество пар входных и выходных сигналов для линейного канала образует гиперплоскость, погруженную в пространство представления с координатными осями $\bar{y}_1, \bar{y}_2, ..., \bar{y}_n$. При этом гиперплоскость имеет собственную систему координат $\bar{x}_1, \bar{x}_2, ..., \bar{x}_n$. Каждая точка гиперплоскости одновременно отображает и входной, и выходной сигналы. Временные отсчеты выходного сигнала, образующие вектор $\bar{s}_{вых}$, это координаты точки в системе координат $\bar{y}_1, \bar{y}_2, ..., \bar{y}_n$, а отсчеты входного сигнала, образующий вектор $\bar{s}_{вх}$, – координаты точки в собственной системе координат гиперплоскости $\bar{x}_1, \bar{x}_2, ..., \bar{x}_n$.

На рис. 1 приведен наглядный пример двумерной плоскости, погруженной в трехмерное пространство представления с координатными осями $\bar{y}_1, \bar{y}_2, \bar{y}_3$.

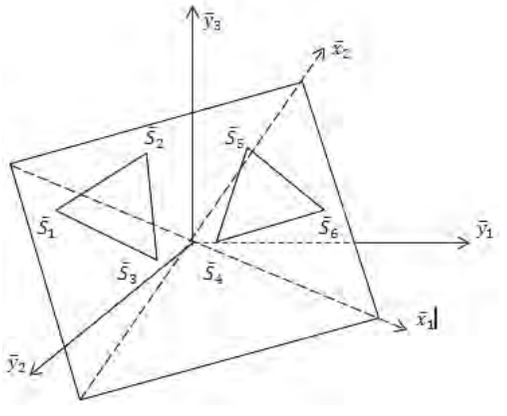

Рис. 1. Простейший пример геометрической (тензорной) модели линейного канала

Изображенные на рис. 1 сигнальные точки $\bar{S}_1, \bar{S}_2, ..., \bar{S}_6$ отображают и двухотсчетные входные сигналы $\bar{S}_{1вх}, \bar{S}_{2вх}, ..., \bar{S}_{6вх}$ (отсчеты этих сигналов – координаты точек в системе координат $\bar{x}_1, \bar{x}_2$), и трехотсчетные выходные сигналы $\bar{S}_{1вых}, \bar{S}_{2вых}, ..., \bar{S}_{6вых}$ (отсчеты этих выходных сигналов – координаты точек в системе координат $\bar{y}_1, \bar{y}_2, \bar{y}_3$).

Размерность гиперплоскости модели канала в данном примере $m = 2$, что определяется числом отсчетов во входных сигналах. Величина $n = 3$ соответствует использованию канала с импульсной реакцией, состоящей из $l = 2$ отсчетов g_1 и g_2. В общем случае $n = m + l - 1$, что следует из соотношения размерностей матриц в матричном аналоге интеграла свертки входного сигнала с импульсной реакцией канала, используемого для расчета выходного сигнала:

$$\bar{s}_{вх} G = \left\| s_{1вх} \quad s_{2вх} \right\| \times \begin{Vmatrix} g_1 & g_2 & 0 \\ 0 & g_1 & g_2 \end{Vmatrix} = \\ = \left\| s_{1вых} \quad s_{2вых} \quad s_{3вых} \right\| = \bar{s}_{вых}, \qquad (1)$$

где $s_{1вх}, s_{2вх}, s_{1вых}, s_{2вых}, s_{3вых}$ – отсчеты входного и выходного сигналов; G – матрица оператора линейного канала, составленная из отсчетов импульсной реакции канала.

Как показано в [3], равенство (1) выполняется для любого исходного базиса, то есть множество пар входных и выходных сигналов образуют гиперплоскость, свойства которой не зависят от базиса, используемого для представления векторов сигналов. Это означает, что гиперплоскость модели линейного канала является тензором [5] и на рис. 1 изображена тензорная модель линейного канала.

Теперь построим на базисных векторах $\bar{x}_1, \bar{x}_2, ..., \bar{x}_m$ гиперплоскости m-мерный параллелепипед, образуемый множеством точек $\bar{S}$, для которых их радиус вектор $\overline{OS}$ разлагается по векторам $\bar{x}_1, \bar{x}_2, ..., \bar{x}_m$ с коэффициентами $\bar{a}_1, \bar{a}_2, ..., \bar{a}_m$, меняющимися непрерывно от 0 до 1. В частных случаях, когда $m = 1$, этот параллелепипед является одномерным отрезком, для $m = 2$ – параллелограммом на двумерной плоскости, при $m = 3$ – параллелепипедом в обычном смысле.

Известно [5], что объем V для m-мерного параллелепипеда может быть выражен модулем определителя матрицы, составленной из координат векторов, на которых построен параллелепипед:

$$V = \det \begin{vmatrix} x_{11} & x_{12} & \cdots & x_m \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mm} \end{vmatrix}. \qquad (2)$$

При переходе в координатную систему $\bar{y}_1, \bar{y}_2, ..., \bar{y}_n$ новое значение объема параллелепипеда V' согласно [5] будет равно $V' = V\, det|P|$, где P – матрица оператора преобразования систем координат, элементы которой равны $p_{ij} = \frac{\partial \bar{y}_i}{\partial \bar{x}_j}$. Можно показать, что в нашем случае $P = G$, откуда следует $V' = V\, det|G|$, что эквивалентно $\frac{V'}{V} = det|G|$. При построении на базисных векторах $\bar{x}_1, \bar{x}_2, ..., \bar{x}_n$ двух m-мерных параллелепипедов с разными объемами V_1 и V_2 можно записать $\frac{V_1'}{V_1} = det|G|$, $\frac{V_2'}{V_2} = det|G|$. Из этих отношений следует

$$\frac{V_2}{V_1} = \frac{V_2'}{V_1'}. \qquad (3)$$

В качестве базисных векторов гиперплоскости модели линейного канала можно использовать любую систему линейно независимых векторов, в том числе и векторы входных сигналов. Тогда (3) можно интерпретировать как свойство линейных каналов сохранять отношение объемов параллелепипедов, образуемых векторами входных сигналов, при преобразовании сигналов каналами связи. Иначе говоря, (3) является формой записи обобщенного инварианта.

Обобщенность этого инварианта заключается в том, что при $m = 1$ формула (3) будет выражать известный инвариант линейного канала в форме сохраняющегося отношения длин однонаправленных векторов входных сигналов [3]. При $m = 2$ имеет место сохранение отношения площадей фигур, расположенных в сигнальном пространстве на двумерной плоскости.

Так как сдвиг в сигнальном пространстве не меняет длин отрезков прямых, площадей и объемов геометрических объектов, то (3) будет справедливо и без «привязки» этих объектов к расположению начала координат. Для иллюстрации этого утверждения на рис. 1 изображены два треугольника, образованные двумя тройками сигнальных точек $\bar{S}_1, \bar{S}_2, \bar{S}_3$ и $\bar{S}_4, \bar{S}_5, \bar{S}_6$. Отношение площадей этих треугольников на выходе канала связи, где они будут отображаться тройками выходных сигналов $\bar{S}_{1вых}, \bar{S}_{2вых}, \bar{S}_{3вых}$ и $\bar{S}_{4вых}, \bar{S}_{5вых}, \bar{S}_{6вых}$, будет равно отношению их площадей, когда они представлены тройками входных сигналов $\bar{S}_{1вх}, \bar{S}_{2вх}, \bar{S}_{3вх}$ и $\bar{S}_{4вх}, \bar{S}_{5вх}, \bar{S}_{6вх}$.

Обобщенный инвариантный метод передачи сообщений по линейным каналам связи

На основе обобщенного инварианта линейных каналов (3) можно реализовать алгоритмы инвариантной модуляции и демодуляции, которые в «укрупненном» виде имеют следующую форму:

- модуляция – $V_i = I_i V_{on}$,
- демодуляция – $\hat{I}_i = \frac{\hat{V}_i'}{\hat{V}_{on}'}$, (4)

где I_i – значение передаваемого информационного элемента сообщения; V_{on} – объем m-мерного «опорного» параллелепипеда, образованного набором опорных сигналов на входе канала; V_i – объем m-мерного «информационного» параллелепипеда, образованного i-ым набором информационных сигналов, передающих значение i-го информационного элемента; верхним знаком «^» обозначены оценки этих величин на выходе канала связи.

Рассмотрим пример реализации обобщенных алгоритмов модуляции и демодуляции (4). Для геометрической наглядности, как и ранее, используем двухотсчетные входные сигналы (m = 2), трехотсчетные выходные сигналы (n = 3), что соответствует двухотсчетной импульсной реакции канала (l = 2). В качестве обобщенного инварианта выберем отношение площадей «информационных» и «опорного» треугольников. Пусть опорный треугольник, образованный тремя сигналами $\bar{S}_1, \bar{S}_2, \bar{S}_3$, имеет площадь S_{on} (см. рис. 1). Для формирования «информационного» треугольника с площадью $S_i = I_i S_{on}$ необходимо определить три соответствующих сигнала $\bar{S}_{1i}, \bar{S}_{2i}, \bar{S}_{3i}$. Очевидно, этот выбор можно сделать множеством способов, что положительно влияет на информационную защищенность обобщенного инвариантного метода передачи.

Простой способ формирования информационного треугольника из опорного треугольника использует известное свойство определителя матрицы: умножение элементов какой-либо строки (столбца) матрицы на число изменяет пропорционально этому числу величину определителя матрицы [6]. В нашем случае площадь опорного треугольника равна определителю матрицы, составленной из координат векторов трех опорных сигналов $\bar{S}_1, \bar{S}_2, \bar{S}_3$:

$$S_{on} = \frac{1}{2}\begin{vmatrix} x_{11} & x_{21} & 1 \\ x_{12} & x_{22} & 1 \\ x_{13} & x_{23} & 1 \end{vmatrix},$$

где x_{1i} и x_{2j} – координаты векторов соответствующих сигналов, образующих опорный треугольник. Этими координатами в рассматриваемом примере являются временные отсчеты входных сигналов.

Итак, для формирования информационного треугольника с площадью $S_i = I_i S_{on}$ необходимо вычислить три информационных сигнала, представленных векторами $\overline{S}_{1i}, \overline{S}_{2i}, \overline{S}_{3i}$. Используя упомянутое выше свойство определителя, выполнение равенства $S_i = I_i S_{on}$ можно обеспечить, если координаты векторов $\overline{S}_{1i}, \overline{S}_{2i}, \overline{S}_{3i}$ будут удовлетворять следующему соотношению:

$$S_{1i} = \left\| I_i' x_{11};\quad I_i'' x_{21} \right\|; S_{2i} = \left\| I_i' x_{12};\quad I_i'' x_{22} \right\|;$$
$$S_{3i} = \left\| I_i' x_{13};\quad I_i'' x_{23} \right\|. \qquad (5)$$

При этом должно быть $I_i' I_i'' = I_i$. В частных случаях $I_1' = I_i$, тогда $I_1'' = 1$ и, наоборот, $I_1'' = I_i$, $I_1' = 1$.

Выражение (5) описывает простую реализацию обобщенного инвариантного метода модуляции, когда в качестве обобщенного инварианта линейных каналов используется отношение площадей треугольников, образуемых тройками передаваемых сигналов.

Алгоритм демодуляции, как это следует из (4), состоит из двух операций: вычисление оценок площадей информационного и опорного треугольников, образуемых тройками выходных сигналов, и расчет отношения площадей. В нашем примере оценки площадей опорного и информационных треугольников можно вычислить по формуле [6]:

$$\hat{S}_{\Delta} = \frac{1}{2}\left\{ \begin{vmatrix} y_{11} & y_{31} & 1 \\ y_{12} & y_{32} & 1 \\ y_{13} & y_{33} & 1 \end{vmatrix}^2 + \begin{vmatrix} y_{31} & y_{11} & 1 \\ y_{32} & y_{12} & 1 \\ y_{33} & y_{13} & 1 \end{vmatrix}^2 + \begin{vmatrix} y_{11} & y_{21} & 1 \\ y_{12} & y_{22} & 1 \\ y_{13} & y_{23} & 1 \end{vmatrix}^2 \right\}^{\frac{1}{2}},$$

где y_{ij} – координаты векторов выходных сигналов в системе координат $\overline{y}_1, \overline{y}_2, \overline{y}_3$ пространства представления. У нас y_{ij} – это i-ый временной отчет (i = 1; 2; 3) j-го сигнала из тройки выходных сигналов, образующих опорный или информационный треугольники. Разумеется, приведенные выражения обобщаются и на случай сигнальных пространств больших размерностей.

Оценка информационной защищенности обобщенного инвариантного метода передачи сообщений

Многовариантность способов формирования опорных и информационных сигнальных m-мерных параллелепипедов в обобщенном инвариантном методе передачи сообщений открывает широкие возможности для обеспечения информационной безопасности системы связи. Далее оценим информационную защищенность рассмотренного в примере метода передачи с использованием обобщенного инварианта в форме отношения площадей информационных и опорного треугольников.

Пусть сообщение передается блоками длиной z информационных элементов I_i, а в качестве обобщенного инварианта используется отношение площадей информационных и опорного треугольников. Тогда блок будет передан тремя опорными и $3z$ информационными сигналами. Предположим, что третьей стороне известен метод передачи сообщений. Так как величина площади опорного сигнального треугольника используется при вычислении оценки каждого принимаемого информационного элемента, то защита передаваемых сообщений от несанкционированного доступа может быть затруднена посредством маскирования сигналов опорного треугольника.

Для маскирования опорных сигналов можно воспользоваться тремя последовательными процедурами. Первая процедура разделяет каждый из трех опорных сигналов на последовательность из r сигналов-слагаемых. Назначение второй процедуры – умножение каждого из r слагаемого на некоторое секретное число из множества чисел размером K. Последняя процедура – перестановка во времени преобразованных $3r$ слагаемых опорных сигналов и $3z$ информационных сигналов. Тогда общее число возможных вариантов маскирования опорных сигналов равно $N_{общ} = C_{3z}^{3r} K^{3r}$.

Если, например, z = 100, r = 5, K = 10, то $N_{общ} > 2^{140}$. При таких же значениях z, r, K инвариантный метод передачи значений информационных элементов отношением длин однонаправленных векторов сигналов обеспечивает число вариантов маскирования опорного сигнала $2^{26} < N_{общ} < 2^{27}$ [7]. Для сравнения отметим, что стандарт шифрования DES имеет 2^{56} вариантов криптопреобразований.

Выводы

Обобщенный инвариантный метод передачи позволяет использовать набор сигналов, не ограниченный условием подобия их форм, как это имеет место в частном случае при передаче сообщений отношением длин однонаправленных векторов сигналов. Разнообразие форм используемых сигналов способствует существенному увеличению информационной защищенности передаваемых сообщений по сравнению с упомянутым выше методом. Необходимы дальнейшие исследования обобщенного метода передачи сообщений с целью анализа его помехозащищенности.

Литература

1. Окунев Ю.Б.Системы связи с инвариантными характеристиками помехоустойчивости. М.: Связь, 1973. – 80 с.
2. Лебедянцев В.В. Принцип симметрии и синтез системы передачи информации // Материалы ВНТК «Применение методов теории информации для повышения эффективности и качества радиоэлектронных систем». М.: Радио и связь, 1984. – С. 78
3. Лебедянцев В.В. Разработка и исследование методов анализа и синтеза инвариантных систем связи. Дисс. д.т.н. Новосибирск, 1995.
4. Ибрагимов М.Х. Группы преобразований в математической физике. М.: Наука, 1983. – 280 с.
5. Рашевский П.К. Риманова геометрия и тензорный анализ. М.: Наука, 1964. – 664 с.
6. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М.: Наука, 1974. – 832 с.
7. Лебедянцев В.В., Морозов Е.В. Оценки информационной защищенности и помехоустойчивости инвариантной системы связи // Доклады ТГУСУР. Ч.1, №1(21), 2010. – С. 152-155.

GENERALIZEDINVARIANT METHODMESSAGING ANDASSESSMENT OF ITSINFORMATION SECURITY

Lebedyantsev V.V.

In work the generalized invariant of linear communication channels in the form of the rela-tion of volumes of the m-dimensional parallelepipeds formed in alarm space by the relevant groups of transmitted signals kept by channels is synthesized. The algorithm of transmission of messages using this invariant is developed. The assessment of information security of the generalized invariant method of transmission of messages is given.

Keywords: *group of transformations, the invariant, the generalized invariant method of transfer, information security.*

Лебедянцев Валерий Васильевич, д.т.н., профессор, заведующий Кафедрой автоматической электросвязи Сибирского государственного университета телекоммуникаций и информатики (г. Новосибирск). Тел. (8-383) 269-82-42; 8-913-010-73-01. E-mail: lebvv@sibsutis.ru

УДК691.396

МОДЕЛИРОВАНИЕ СИСТЕМЫ MIMO В КАНАЛЕ С ПАМЯТЬЮ

Коняева О.С.

В статье рассматривается система MIMO 2×2 в канале связи с памятью. Были получены оценки достоверности принятой последовательности символов (BER) для различных алгоритмов, компенсирующих помехи и искажения сигнала, – алгоритм сведения к нулю (ZF) и алгоритм наименьших квадратов (MMSE). Получены зависимости вероятности ошибки на бит от отношения «сигнал/шум» в месте приема для различной памяти канала.

Ключевые слова: MIMO, алгоритм наименьших квадратов, алгоритм сведения к нулю, битовый коэффициент ошибок, канал с памятью, межсимвольная интерференция.

Введение

В современных высокоскоростных системах передачи дискретных сообщений значительно улучшить емкость сети, спектральную эффективность и скорость передачи информации можно при использовании технологии с многоканальным входом и многоканальным выходом (Multiple Input Multiple Output – MI-MO),