УДК 681.3.067 (075.8)

Обзор и анализ информационной защищенности инвариантных систем связи

В. В. Лебедянцев, М. В. Лебедянцев

Приведен обзор принципов функционирования инвариантных систем связи. Показаны способы обеспечения информационной защищенности в такого рода системах связи. Получены аналитические выражения для оценки их информационной защищенности.

Ключевые слова: канал связи, группа преобразований канала связи и его инварианты, инвариантная система связи, информационная защищенность инвариантной системы связи.

1. Введение

Обеспечение нечувствительности (инвариантности) систем связи к вредному влиянию на передаваемые сигналы неидеальности характеристик тракта передачи, различного рода помех представляет собой одну из основных задач теории и практики связи. Эта задача решается различными методами – коррекцией характеристик канала связи, применением специальных сигналов, помехоустойчивыми методами приема сигналов, помехоустойчивым кодированием, применением обратной связи и т.п.

Однако теория групп преобразований позволяет реализовать прямой метод синтеза инвариантных систем связи. Суть этого метода, по-видимому, впервые была изложена в [1]. В его основе лежит установление того факта, что изменения сигналов-переносчиков информации каналами связи и помехами, действующими в них, описываются соответствующими группами преобразований.

Известно, что каждая группа преобразований обладает набором инвариантов – определенных соотношений между параметрами сигналов, остающимися неизменными при преобразовании каналом самих сигналов. Вследствие этого свойства инвариантов их величины следует использовать для безыскаженной передачи информационных элементов по искажающим сигналы каналам связи.

К настоящему времени синтезированы инварианты для линейных и нелинейных каналов связи, инварианты для каналов с аддитивными помехами. На базе этих инвариантов разработаны инвариантные методы модуляции и демодуляции для систем связи, использующих такого типа каналы связи [2]. Системы связи, в которых применяются такие виды модуляции и демодуляции, называются инвариантными.

Следует отметить, что одной из первых инженерных разработок инвариантной системы связи является система с относительной фазовой модуляцией. В качестве инварианта в ней используется разность фаз двух соседних гармонических сигналов, которая не зависит от знака коэффициента передачи канала связи. Упрощенно можно считать, что группа преобразований канала здесь включает в себя две операции: умножение сигналов на +1 и –1. Эти операции одновременно являются нейтральными и обратными элементами группы преобразований и обеспечивают свойство замкнутости.

Поскольку в настоящее время проблема обеспечения безопасной передачи сообщений по каналам связи приобретает все большее значение, представляет теоретический и практический интерес анализ информационной защищенности инвариантных систем связи.

2. Анализ информационной защищенности двух инвариантных систем передачи информации для линейных каналов связи

Под защищенностью системы связи будем понимать способность системы противостоять несанкционированному доступу к конфиденциальной информации, передаваемой по ее каналу.

Задача создания системы защиты передаваемой информации состоит из двух подзадач:

- создание системы защиты;
- оценка надежности разработанной системы защиты.

Рассмотрим решение первой подзадачи.

Как показано в [2], преобразование сигналов в линейном канале связи (в канале, в котором выполняется принцип суперпозиции) описывается аффинной группой преобразований с основным инвариантом в виде так называемого «отношения трех точек». На рис. 1 показана схема аффинного преобразования длин векторов входных сигналов линейным каналом связи.

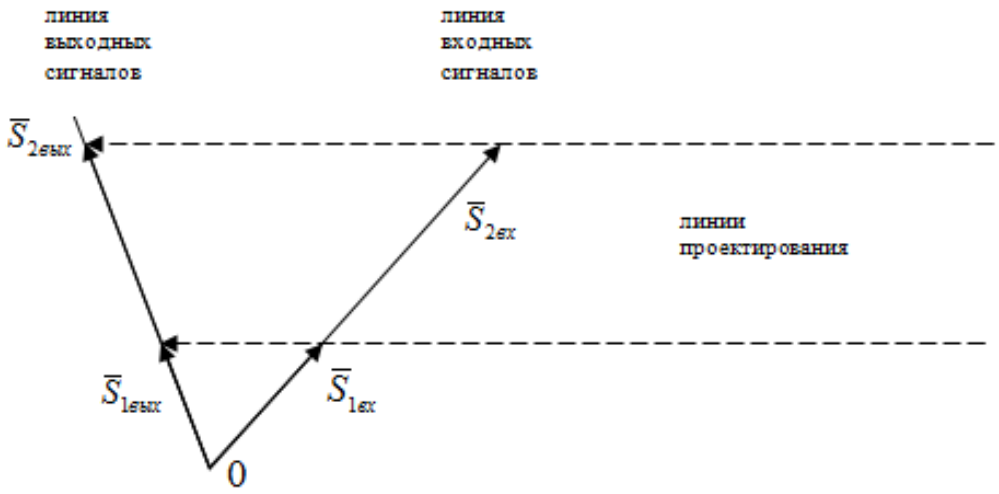

Рис. 1. Схема аффинного преобразования сигналов для линейного канала связи

Основным инвариантом J для данной схемы будет сохраняемое каналом отношение длин векторов сигналов, имеющих подобные формы (векторы которых совпадают по направлению):

$$J = \frac{\left|\overline{S}_{2вх}\right|}{\left|\overline{S}_{1вх}\right|} = \frac{\left|\overline{S}_{2вых}\right|}{\left|\overline{S}_{1вых}\right|} \quad .$$

Из этого выражения можно получить простые алгоритмы инвариантной амплитудной модуляции и демодуляции

$$\overline{S}_{iвх} = J_i \overline{S}_{овх}; \hat{J}_i = \frac{\left|\hat{\overline{S}}_{iвых}\right|}{\left|\hat{\overline{S}}_{овых}\right|} \quad ,$$

где J_i – величина передаваемого информационного элемента;

$\overline{S}_{i\text{вх}}$, $\left|\hat{\overline{S}}_{i\text{вых}}\right|$, $\overline{S}_{о\text{вх}}$, $\left|\hat{\overline{S}}_{о\text{вых}}\right|$ – векторы и оценки длин векторов информационных и опорных сигналов на входе и выходе канала связи.

Здесь предполагается, что информация передается блоками, содержащими *n* сигналов. В начале блока передается опорный сигнал $\overline{S}_{о\text{вх}}$ (на рис. 1 обозначен как $\overline{S}_{1\text{вх}}$). В роли информационных сигналов выступает сигнал $\overline{S}_{2\text{вх}}$.

Система защиты передаваемой информации инвариантной системы связи базируется на возможности маскирования опорного сигнала, которое можно осуществлять разными способами.

Первый способ заключается в обеспечении секретности расположения опорного сигнала внутри блока сигналов. Как дополнительная мера – непрерывная смена позиции опорного сигнала по неизвестному для злоумышленника алгоритму.

Для определения места расположения опорного сигнала внутри блока, состоящего из *n* сигналов, очевидно, потребуется C_n^1 - проб (количество сочетаний из *n* по одному).

Увеличить трудоемкость определения величины опорного сигнала возможно путем разделения его на *m* составляющих, занимающих внутри блока секретные местоположения. При это количество вариантов размещения *m* составляющих опорного сигнала составит C_n^m.

Наконец, еще более увеличивает трудоемкость определения величины опорного сигнала использование *m* секретных множителей a_j $(1 \le j \le m)$, на которые умножаются составляющие опорного сигнала. При этом вектор маскированного опорного сигнала $\overline{S}_{омаск}$, состоящий из *n* элементов, *n*−*m* из которых «нулевые», а *m* заполнены ненулевыми составляющими, можно рассчитать следующим образом

$$\overline{S}_{омаск} = \overline{S}_{сост} А П ,$$

где $\overline{S}_{сост}$ – матрица-строка, содержащая *m* элементов, каждый из которых равен $\left|\overline{S}_{о\text{вх}}\right| / m$;

А – диагональная матрица размера *m*m,* диагональные элементы которых равны секретным значениям множителей a_j;

П – матрица секретной перестановки составляющих опорного сигнала внутри блока сигналов.

Матрица *П* имеет *m* строк и *n* столбцов и состоит из единиц и нулей. При этом номер строки, в которой расположена единица, указывает номер составляющей опорного сигнала, а номер столбца – местоположение внутри блока.

На приемной стороне восстановление вектора опорного сигнала осуществляется посредством обратных математических операций:

$$\hat{\overline{S}}_{сост} = \hat{\overline{S}}_{омаск} П^T A^{-1}$$ (Т – символ транспонирования).

Вычисление оценки длины вектора опорного сигнала на приемной стороне производится суммированием элементов $\hat{\overline{S}}_{сост}$.

Очевидно, что ключевой информацией в данном методе обеспечения информационной защищенности инвариантной системы связи является набор диагональных элементов матрицы *А* и структура матрицы перестановки *П*. Для взлома этой ключевой информации «методом грубой силы» потребуется количество операций перебора равное

$$N = C_n^m K^m ,$$

где K – число возможных значений, которые могут иметь коэффициенты a_j.

Дальнейшее увеличение сложности маскирования опорного сигнала возможно благодаря перестановке составляющих опорного сигнала в той группе, которая образована вариантом сочетания из n элементов по m. В этом случае количество операций перебора возрастает и будет определяться уже количеством размещений из n по m:

$$N = D_n^m * K^m,\ D_n^m = n(n-1)(n-2)...[n-(m-1)].$$

3. Анализ информационной защищенности инвариантной системы, использующей обобщенный инвариант линейного канала

В [3] синтезирован обобщенный инвариант линейных каналов связи в виде сохраняемого каналами отношения объемов многомерных параллелепипедов, образуемых в сигнальном пространстве соответствующими группами передаваемых сигналов. Для иллюстрации на рис. 2 в сигнальном пространстве входных сигналов (двумерная плоскость) изображены два «сигнальных» треугольника, сформированные двумя тройками векторов входных сигналов $\bar{S}_1, \bar{S}_2, \bar{S}_3$ и $\bar{S}_4, \bar{S}_5, \bar{S}_6$ соответственно.

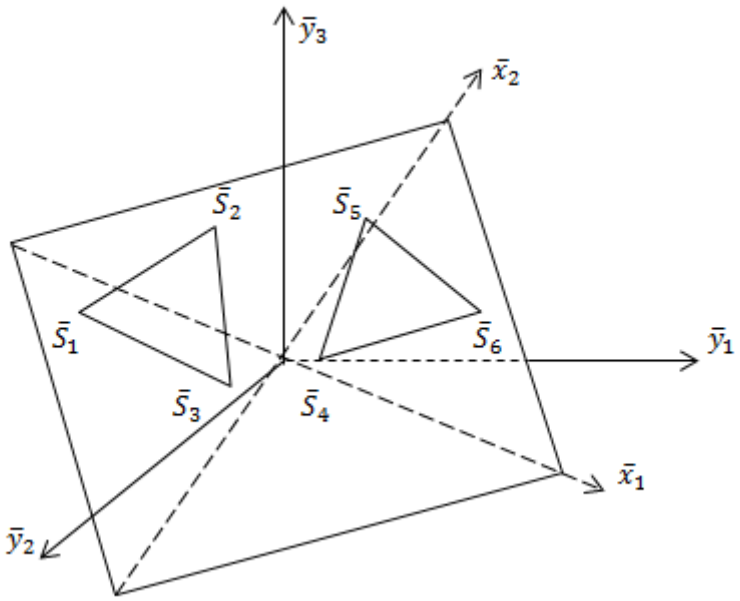

Рис. 2. Сигнальное пространство входных и выходных сигналов

Для обеспечения геометрической наглядности на рисунке изображены входные сигналы, векторы которых представлены в базисе $\bar{x}_1$ и $\bar{x}_2$. В частности, в роли базисных функций $\bar{x}_1(t)$ и $\bar{x}_2(t)$ можно рассматривать функции Котельникова. Тогда сигналы $S_1(t) \div S_6(t)$ будут двухотсчетными сигналами. В случае, когда импульсная реакция канала представлена также двумя отчетами, выходные сигналы будут отображаться тремя отчетами. При этом для отображения векторов выходных сигналов необходимо использовать трехмерное пространство с координатными осями $\bar{y}_1$, $\bar{y}_2, \bar{y}_3$.

Обозначим площади треугольников $\Delta\bar{S}_1\bar{S}_2\bar{S}_3 = \mathbf{S_1}$, а $\Delta\bar{S}_4\bar{S}_5\bar{S}_6 = \mathbf{S_2}$. Как показано в [3], для любого линейного канала выполняется равенство

$$\frac{\mathbf{S_2}}{\mathbf{S_1}} = \frac{\mathbf{S_2'}}{\mathbf{S_1'}},$$

где $\mathbf{S_2'}$ и $\mathbf{S_1'}$ – площади сигнальных треугольников, образованных соответствующими выходными сигналами.

В данном примере сигнальные треугольники являются частным случаем многомерных параллелепипедов.

При использовании обобщенного инварианта алгоритмы инвариантной модуляции и демодуляции будут иметь вид $\mathbf{S_{2i}} = J_i \mathbf{S_1}, \hat{J}_i = \frac{S'_{2i}}{S'_1}$.

Теперь в роли опорного и информационных сигнальных объектов выступают *R*-сигнальные конструкции (*R* – количество сигналов, определяющих размер и форму опорного и сигнального объектов). При этом, очевидно, длина сигнального блока, переносящего *n* информационных элементов будет равна *(n+1)R*.

Для рассматриваемого инвариантного метода передачи можно рассчитать общее количество вариантов маскирования опорных сигнальных конструкций:

$N = C^{Rm}_{R(n+1)} K^{Rm}$, $C^{Rm}_{R(n+1)}$ – число сочетаний из *R(n+1)* элементов по *Rm*.

К примеру, если *R=3,n*=100, *m*=5, *K*=10, то $N > 2^{140}$.

При таких же значениях *n*, *m* и *K* инвариантный метод передачи значений информационных элементов отношением длин однонаправленных векторов сигналов обеспечивает число вариантов маскирования опорного сигнала $2^{26} < N < 2^{27}$.

Для сравнения отметим, что стандарт шифрования DES имеет 2^{56} вариантов криптопреобразований.

Следует добавить, что и при данном методе инвариантной передачи возможно использование перестановок составляющих опорного сигнала внутри группы, образованной конкретным вариантом сочетания из *R(n+1)*элементов по *Rm*. Тогда в предыдущей формуле число сочетаний следует заменить на число размещений $D^{Rm}_{R(n+1)}$.

4. Анализ информационной защищенности инвариантной системы связи по нелинейному каналу связи

Аффинная группа преобразований, описывающая преобразования сигналов линейными каналами связи, является подгруппой более общей группы проективных преобразований. Схема проективного преобразования векторов сигналов представлена на рис. 3.

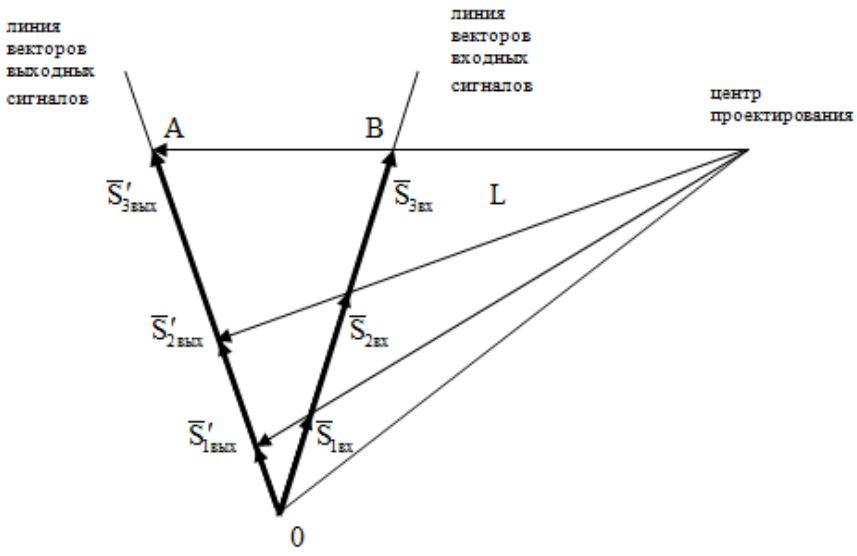

Рис. 3. Проективная схема преобразования длин векторов сигналов нелинейным каналом связи

При использовании предположения о том, что динамические диапазоны длин векторов входных и выходных сигналов совпадают и равны d, т.е. ΔAOB – равнобедренный, можно получить следующую нелинейную зависимость длин векторов выходных сигналов от длин векторов входных сигналов

$$\left|\overline{S}_{вых}\right| = d - \frac{(d - \left|\overline{S}_{вх}\right|)(2d \sin\frac{\alpha}{2} + L)}{2(d - \left|\overline{S}_{вх}\right|)\sin\frac{\alpha}{2} + L)}, \qquad (1)$$

где L – расстояние от центра проектирования до линии входных сигналов;
α – угол между линиями входных и выходных сигналов.

Нетрудно убедиться, что (1) описывает множество как вогнутых, так и выпуклых амплитудных характеристик нелинейного канала, а при $L \to \infty$ будет иметь место схема аффинного преобразования (рис.1).

Известно, что группа проективных преобразований имеет инвариант в форме «ангармонического отношения четырех точек», который при обозначениях на рис. 3 примет вид

$$\frac{\left|\overline{S}_{1вх}\right|}{\left|\overline{S}_{3вх}\right|} : \frac{\left|\overline{S}_{2вх}\right| - \left|\overline{S}_{1вх}\right|}{\left|\overline{S}_{3вх}\right| - \left|\overline{S}_{2вх}\right|} = \frac{\left|\overline{S}_{1вых}\right|}{\left|\overline{S}_{3вых}\right|} : \frac{\left|\overline{S}_{2вых}\right| - \left|\overline{S}_{1вых}\right|}{\left|\overline{S}_{3вых}\right| - \left|\overline{S}_{2вых}\right|}, \qquad (2)$$

При использовании в качестве информационного сигнала $S_1(t)$, отображаемого вектором $\overline{S}_{1вх}$, а в качестве опорных сигналов $S_2(t)$ и $S_3(t)$, представленных векторами $\overline{S}_{2вх}$ и $\overline{S}_{3вх}$, из (2) можно получить алгоритмы нелинейных инвариантных амплитудных модуляции и демодуляции, которые будут работоспособны для любого нелинейного канала, амплитудная характеристика которого удовлетворяет (1):

$$\left|\overline{S}_i\right| = \frac{J_i \left|\overline{S}_2\right| \left|\overline{S}_3\right|}{\left[S_3(1 + J_i) - S_2\right]} \text{ – модуляция;}$$

$$\hat{J}_i = \frac{\left|\hat{\bar{S}}_{i\,вых}\right|}{\left|\hat{\bar{S}}_{3вых}\right|} : \frac{\left|\hat{\bar{S}}_{2вых}\right| - \left|\hat{\bar{S}}_{i\,вых}\right|}{\left|\hat{\bar{S}}_{3вых}\right| - \left|\hat{\bar{S}}_{2вых}\right|} \text{ – демодуляция.}$$

При оценке информационной защищенности инвариантной системы связи по нелинейному каналу следует иметь ввиду, что разделение опорных сигналов на составные части, как это описано выше, неприемлемо, так как для нелинейного канала принцип суперпозиции не выполняется. В этой связи маскирование двух опорных сигналов возможно лишь за счет секретной процедуры их размещения внутри блока сигналов. При этом количество возможных размещений, очевидно, будет равно $N=n(n-1)$.

Таким образом, информационная защищенность инвариантной системы связи по нелинейному каналу уступает информационной защищенности инвариантной системы связи для линейного канала.

5. Заключение

Инвариантные системы связи имеют внутренние возможности для обеспечения информационной защищенности передаваемой информации. Эти возможности базируются на различных способах маскирования опорных сигналов, передаваемых внутри блока информационных сигналов.

Наиболее сложными механизмами маскирования обладают инвариантные системы связи по линейным каналам связи, среди которых с позиций криптостойкости выделяется система передачи, использующая обобщенный инвариант линейных каналов.

Полученные аналитические выражения для расчета трудоемкости определения опорных сигналов позволяют находить необходимые значения параметров маскирования опорных сигналов.

Литература

1. *Лебедянцев В. В.* Применение теории групп преобразований для оптимизации систем связи. // Всесоюзный науч.-тех. семинар «Качество функционирования и надежность систем автоматической коммутации и сетей электросвязи»: Сб. докл. Новосибирск, 1988. С. 21.
2. *Лебедянцев В. В.* Разработка и исследование методов анализа и синтеза инвариантных систем связи. Диссертация на соискание ученой степени доктора технических наук. Новосибирск, 1995.
3. *Лебедянцев В. В.* Обобщенный инвариантный метод передачи сообщений и оценка его информационной защищенности // Инфокоммуникационные технологии. 2014. №3. С. 28–32.

Статья поступила в редакцию 04.02.2016

Лебедянцев Валерий Васильевич
д.т.н., профессор, заведующий кафедрой автоматической электросвязи СибГУТИ, ул. Кирова 86, тел. (383) 2-698-242, e-mail: lebvv@sibsutis.ru.

Лебедянцев Максим Валерьевич
аспирант кафедры передачи дискретных сообщений и метрологии СибГУТИ, ул. Кирова 86, тел. 8-923-158-86-55, e-mail: mlebedyantsev@gmail.com.

Review and information security analysis of invariant communication systems

V.V. Lebedyantsev, M.V. Lebedyantsev

In this article, an overview of the principles of invariant communication systems functioning is provided. The methods of ensuring information security in such communication systems are presented. Analytical expressions for evaluation of its information security are derived.

Keywords: channel, the group of communication channel transformations and its invariants, invariant communication system, information security of invariant communications system.