ОЦЕНКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМЫ СВЯЗИ С ИНВАРИАНТНОЙ НЕЛИНЕЙНОЙ АМПЛИТУДНОЙ МОДУЛЯЦИЕЙ

В. В. Лебедянцев

Сибирский государственный университет телекоммуникаций и информатики, 630102, Новосибирск, Россия

УДК 621.393

Описывается принцип работы нового типа системы связи, использующей для безыскаженной передачи сообщений инварианты канала связи. Рассматривается инвариантная система передачи через каналы связи, характеризуемые проективной группой преобразований. К каналам такого рода относятся линейные каналы и широкий подкласс нелинейных каналов. Применение в таких системах служебных сигналов позволяет обеспечить криптографическую защиту передаваемых сообщений путем изменения специальным секретным способом структуры служебных сигналов. Проведена оценка криптостойкости инвариантного метода передачи.

Ключевые слова: инвариант канала связи, инвариантная система связи, информационная безопасность.

In article the new type of an invariant communications system is described. Invariant systems for message transfer use invariants communication channel. The information security of invariant communication system is estimated.

Key words: invariant of channel communication, invariant of system communication, information security.

Инвариантные системы связи [1] представляют собой новый класс систем передачи информации. Их новизна обусловлена тем, что для передачи значений информационных элементов используется новая форма представления информации – инварианты группы преобразований, характеризующей применяемый канал связи.

Математическое обоснование нового метода передачи информации базируется на описании преобразований сигналов каналом в виде преобразования системы координат, в которой представляются векторы сигналов. Как показано в [1], множество выходных сигналов канала связи удовлетворяет уравнению плоскости, если канал линейный, или уравнению криволинейной поверхности, если канал нелинейный. Изменяя спектральные коэффициенты входных сигналов, на поверхности множества выходных сигналов можно построить собственную систему координат. При этом спектральные коэффициенты входного сигнала будут определять координаты сигнальной точки в собственной системе координат поверхности, а спектральные коэффициенты выходного сигнала – координаты сигнальной точки в системе координат пространства представления выходных сигналов. В этом пространстве отображается поверхность множества выходных сигналов.

Основываясь на данной геометрической модели канала связи в виде поверхности, состоящей из сигнальных точек, преобразование сигналов каналом можно рассматривать как преобразование G^{T} собственной системы координат $\{\boldsymbol{\varphi}_i\}$ поверхности сигнальных точек в систему координат $\{\boldsymbol{\Psi}_i\}$ пространства представления выходных сигналов:

$$\|\boldsymbol{\Psi}_i\| = G^{\mathrm{T}} \|\boldsymbol{\varphi}_i\| .$$

При этом преобразование вектора спектральных коэффициентов входного сигнала $\mathbf{S}_{\text{вх}}$ в вектор спектральных коэффициентов выходного сигнала $\mathbf{S}_{\text{вых}}$ описывается формулой

$$\mathbf{S}_{\text{вых}} = \mathbf{S}_{\text{вх}} G$$

для линейного канала и

$$\mathbf{S}_{\text{вых}} = \mathbf{S}_{\text{вх}} G(\mathbf{S}_{\text{вх}})$$

для нелинейного канала.

Матрица оператора преобразования G определяется свойствами канала связи, например отсчетами импульсной реакции линейного канала [1].

Как известно, преобразование системы координат является примером группы преобразований [2]. "Элементами" группы преобразований являются "действия", например: вращение, растяжение, сжатие, сдвиг и т. д. Среди множества групп преобразований наиболее хорошо изученными являются группа вращений (группа ортогональных преобразований), аффинная группа преобразований и группа проективных преобразований. Среди перечисленных групп наиболее общей является группа проективных преобразований, включающая в качестве подгруппы группу аффинных преобразований. В свою очередь, группа аффинных преобразований в качестве подгруппы включает группу ортогональных преобразований.

В работе [1] показано, что группа аффинных преобразований описывает преобразования сигналов линейными каналами, а группа проективных преобразований – преобразования длин векторов сигналов в широком подклассе нелинейных каналов с амплитудными характеристиками следующего вида:

$$\left|\mathbf{S}_{\text{вых}}\right| = l\left|\mathbf{S}_{\text{вх}}\right| \Big/ \left(D - l - \left|\mathbf{S}_{\text{вх}}\right|\right)$$

(l – параметр D-диапазона значений модулей векторов входных сигналов).

Группы преобразований обладают набором инвариантов – величин, сохраняющихся при действии преобразований группы [2]. Так, группа ортогональных преобразований, описывающая вращения векторов, имеет основной инвариант в виде длины вектора. Более общая группа аффинных преобразований обладает основным инвариантом в форме отношения трех точек. Этот инвариант означает, что отношения длин отрезков, лежащих на одной прямой, сохраняются при любых поворотах и сжатиях (растяжениях) этой прямой. Наконец, основным инвариантом проективной группы преобразований является ангармоническое отношение четырех точек [2].

Следует отметить, что инварианты более общей группы преобразований являются инвариантами подгрупп этой группы. Так, ангармоническое отношение четырех точек является инвариантом не только проективной группы, но и аффинной и ортогональной групп преобразований.

Очевидно, в силу своей неизменности относительно преобразований сигналов каналом связи инварианты являются идеальной формой представления значений информационных элементов, обеспечивающей неискаженную передачу информации через искажающие сигналы каналы связи.

В канале связи сигналы искажаются не только элементами канала (средой передачи, фильтрами и т. д.), но и мультипликативными и аддитивными помехами. Искажения сигналов помехами также можно описать соответствующими группами преобразований, обладающими собственными инвариантами. Используя инварианты всех групп преобразований, характеризующих канал связи, можно обеспечить неискаженную передачу информации. Исключением из общего правила является помеха типа белого шума, влияние которой в силу ее особых свойств полностью устранить нельзя. Однако, применяя методы оптимальной обработки сигналов, воздействие белого шума на качество передачи информации можно существенно уменьшить.

С использованием инвариантов линейного канала в [1] была синтезирована инвариантная амплитудная модуляция (ИАМ). Оценка устойчивости инвариантной системы связи с ИАМ к воздействию белого шума выполнена. Как показали исследования, при применении в инвариантной системе

для приема сигналов метода максимального правдоподобия помехоустойчивость близка к потенциальной для неинвариантных систем.

В [1] на основе инварианта проективной группы преобразований – ангармонического отношения четырех точек – синтезирована инвариантная нелинейная амплитудная модуляция (ИНАМ), алгоритмы модуляции и демодуляции которой представлены формулами

$$|\mathbf{S}_i| = \frac{|\mathbf{S}_2|}{1 - J_i\left(|\mathbf{S}_2| - |\mathbf{S}_1|\right)/|\mathbf{S}_2|}; \qquad (1)$$

$$\hat{J}_i = |\hat{\mathbf{S}}_1|\ \left(|\hat{\mathbf{S}}_i| - |\hat{\mathbf{S}}_2|\right)/|\hat{\mathbf{S}}_i|\ \left(|\hat{\mathbf{S}}_2| - |\hat{\mathbf{S}}_i|\right), \qquad (2)$$

где $|\mathbf{S}_1|$, $|\mathbf{S}_2|$ – модули длин векторов двух опорных сигналов, передающихся совместно с информационными сигналами $\mathbf{S}_i$; J_i – передаваемое значение i-го информационного элемента; знак "^" обозначает оценку соответствующих величин на приемной стороне.

Из (1), (2) следует, что алгоритм инвариантной нелинейной амплитудной модуляции существенно сложнее классических видов модуляции, поскольку в нем используются два параметра – длины векторов двух опорных сигналов $\mathbf{S}_1$ и $\overline{\mathbf{S}}_2$. Эту сложность целесообразно использовать для криптографической защиты информации, реализуемой на физическом уровне модели OSI. Оценим потенциальную криптостойкость инвариантной нелинейной амплитудной модуляции.

Пусть информация передается блоками сигналов, содержащих n сигналов. Среди этих сигналов два являются опорными ($\mathbf{S}_1$ и $\mathbf{S}_2$), остальные $n-2$ – информационными $(\mathbf{S}_i)$.

В наиболее простом случае скрытие информации можно обеспечить располагая опорные сигналы секретным образом (неизвестным третьим лицам) среди информационных сигналов. Очевидно, что количество вариантов расположения будет равно числу сочетаний C_n^2. Нетрудно рассчитать это количество при длине блока $n = 1000$: $C_{1000}^2 = 499\,500$.

Можно предложить пути дальнейшего увеличения криптостойкости инвариантной нелинейной амплитудной модуляции, например, осуществлять передачу опорных сигналов с измененными амплитудами. Разумеется, способ изменения амплитуд должен быть известен получателю. Пусть каждый из опорных сигналов может быть умножен на любое число из множества размером K. Очевидно, число возможных комбинаций M опорных сигналов будет равно

$$M = K^2,$$

а общее число вариантов шифрования $N_{\text{общ}}$ составит

$$N_{\text{общ}} = C_n^2 K^2.$$

Следующий способ повышения криптостойкости – разделение каждого опорного сигнала на r отдельных составляющих, каждая из которых может быть умножена на секретное число из множества размером K. Секретность числа означает, что оно должно быть неизвестно третьим лицам (неавторизованным пользователям). Общее число возможных перестановок слагаемых опорных сигналов будет приближенно равно $(C_n^r)^2$. С учетом того, что каждое слагаемое может быть умножено на любое число из множества K, общее количество вариантов шифрования составит

$$N_{\text{общ}} = (C_n^r)^2 K^r.$$

Так, принимая n=1000, r=10, K=10, найдем

$$N_{общ} = (C_{1000}^{10})^2 10^{10} \approx 6{,}94 \cdot 10^{56}.$$

Таким образом, полученное число $N_{\text{общ}}$ означает возможность обеспечения высокого уровня информационной безопасности системы передачи с инвариантной нелинейной амплитудной модуляцией. Для сравнения отметим, что алгоритм шифрования DES реализует только 2^{56} вариантов криптопреобразований.

Список литературы

1. Лебедянцев В. В. Разработка и исследование методов анализа и синтеза инвариантных систем связи: Дис. … д-ра техн. наук. Новосибирск, 1995. 253 с.

2. Ефимов Н. В. Высшая геометрия. М.: Наука, 1978. 576 с.

Лебедянцев Валерий Васильевич – д-р техн. наук, проф., зав. кафедрой автоматической электросвязи СибГУТИ, тел.: (383) 269-82-42; e-mail: lebvv@sibsutis.ru

Дата поступления − 05.08.09