УДК 004.056

О методе защиты информации в инвариантной системе связи

В.В. Лебедянцев

Для инвариантной системы связи с блочной передачей сообщений предложен метод защиты информации, использующий маскирование опорных сигналов. Рассмотрено несколько алгоритмов маскирования. Приведена оценка криптографической стойкости алгоритмов.

Ключевые слова: группа преобразований канала связи, инварианты канала, инвариантная система связи, инвариантная амплитудная модуляция, маскирование опорных сигналов, криптографическая стойкость алгоритма маскирования.

1. Введение

Существуют различные математические методы исследования воздействия на сигналы каналов связи, например, посредством дифференциальных, интегральных уравнений, с помощью преобразований Фурье и т.д. Как показано в [1], перечисленные методы являются частными случаями преобразований аффинной группы [2], описывающей изменения сигналов в линейных каналах связи.

Известно, что группы преобразований обладают набором инвариантов – некоторых величин, остающихся неизменными при любых преобразованиях группы. Так, аффинная группа преобразований обладает основным инвариантом в виде отношения длин векторов, имеющих одинаковые направления. На базе этого инварианта в [1] синтезирована инвариантная амплитудная модуляция (ИАМ):

$$\bar{S}_i = I_i \bar{S}_{on} .$$

Здесь:

I_i – значение передаваемого в *i*-м интервале времени информационного элемента;

$\bar{S}_i$, $\bar{S}_{on}$ – векторы информационного и опорного сигналов.

Алгоритм демодуляции имеет вид:

$$\hat{I}_i = \frac{|\hat{\bar{S}}_i|}{|\hat{\bar{S}}_{on}|},$$

где $\hat{I}_i$ – оценка принятого информационного элемента;

$|\hat{\bar{S}}_i|$ и $|\hat{\bar{S}}_{on}|$ – оценки длин векторов принятых информационного и опорного сигналов.

Преимущество системы связи с ИАМ состоит в возможности безыскажённой передачи сообщений по любым линейным каналам с произвольными частотно-временными характеристиками. Конечно, при практической реализации для минимизации энергетических затрат желательно знать границы пропускания канала и использовать сигналы со спектрами, находящимися внутри этой полосы.

Следует также заметить, что в инвариантных системах связи, как и в других системах, влияние белого шума устранить принципиально невозможно.

Дальнейшим развитием теории инвариантных систем связи является синтез инвариантов для нелинейных каналов связи, характеризуемых проективной группой преобразований, с основным инвариантом в виде «ангармонического отношения четырёх точек» [2]. Посредством этого инварианта в [1] синтезирована инвариантная нелинейная амплитудная модуляция (ИНАМ):

$$|\bar{S}_i| = \frac{|\bar{S}_2|}{1 - \frac{I_i(|\bar{S}_2| - |\bar{S}_1|)}{|\bar{S}_1|}}$$

и соответствующая демодуляция

$$\hat{I}_i = \frac{|\hat{\bar{S}}_2|(|\hat{\bar{S}}_i| - |\hat{\bar{S}}_2|)}{|\hat{\bar{S}}_i|(|\hat{\bar{S}}_2| - |\hat{\bar{S}}_1|)},$$

где $|\bar{S}_1|$, $|\bar{S}_2|$, $\left|\hat{\bar{S}}_1\right|$ и $\left|\hat{\bar{S}}_2\right|$ – длины векторов двух опорных сигналов $S_{1on}(t)$, $S_{2on}(t)$ и оценки длин этих векторов.

Общим для двух разновидностей инвариантных методов модуляции является использование опорных сигналов. От точности оценки длин векторов этих сигналов в существенной степени зависит точность оценок значений информационных элементов. В случае, когда криптоаналитику неизвестна оценка длины вектора опорного сигнала, становится невозможным расчёт оценок значений информационных элементов.

2. Методы маскирования опорных сигналов в инвариантных системах связи

Как следует из алгоритмов инвариантной модуляции, расположение опорных сигналов во времени относительно информационных может быть произвольным: до информационных сигналов, внутри блока информационных сигналов или после.

Это позволяет использовать расположение опорного сигнала во времени для его маскирования. При этом в случае использования одного опорного сигнала число вариантов его расположения в блоке сигналов длиной *n* также равно *n*.

Как следует из алгоритма модуляции (1), оценка длины вектора опорного сигнала в целое число раз (I_i) меньше оценок длин векторов информационных сигналов. Это свойство опорного сигнала может быть использовано для определения его места внутри блока информационных сигналов. Исключение этой возможности реализуются изменением опорного сигнала посредством умножения или деления на некоторое секретное случайное целое число *R*.

Следующей возможностью маскирования опорного сигнала является применение процедуры секретной перестановки не только опорного сигнала, но и информационных сигналов. Пусть передатчик сформировал блок значений амплитуд опорных и информационных сигналов длиной *n*. Пронумеруем последовательно числа в этом блоке, начиная с опорного сигнала: 012345...*n*.

Известно [2], что число *N* всех возможных перестановок *n* чисел равно *N=n!*. При большой длине блока число перестановок может быть вычислено по приближённой формуле Стирлинга

$$n! \cong \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Так, уже при *n*=20 число возможных перестановок приблизительно равно $2.4 \cdot 10^{18}$.

Далее рассмотрим возможность применения составного опорного сигнала, отдельные слагаемые которого расположены внутри блока информационных сигналов секретным способом.

Пусть опорный сигнал состоит из m слагаемых с весовыми коэффициентами a_i. Очевидно, набор коэффициентов a_i можно использовать как дополнительную секретную информацию для повышения криптозащиты данных, передаваемых в инвариантных системах связи.

Нетрудно найти число вариантов комбинаций слагаемых опорного сигнала

$$N_B = C_n^m K^m ,$$

где C_n^m– число сочетаний из n по m;
K – размер множества возможных значений коэффициентов a_i.

Особенностью инвариантной нелинейной амплитудной модуляции является использование двух опорных сигналов. Разумеется, перечисленные выше алгоритмы маскирования опорного сигнала применимы и в данном случае. Однако применение двух опорных сигналов позволяет увеличить число вариантов комбинаций расположения их слагаемых. С учётом того, что каждое слагаемое опорных сигналов может быть умножено на любое число из множества размерностью K, то в случае использования инвариантной нелинейной амплитудной модуляции число вариантов расположения слагаемых опорных сигналов станет равным

$$N_B = (C_n^m)^2 K^m.$$

Так, если n=1000, m=10, K=10, получим

$$N_B = (C_{1000}^{10})^2 10^{10} \approx 6.94 \cdot 10^{56}.$$

Отметим, данное значение числа вариантов расположения слагаемых опорных сигналов существенно превышает количество вариантов криптопреобразований в стандарте шифрования DES, равное 2^{56}. Следует также иметь ввиду дополнительную возможность перестановки информационных сигналов в каждом блоке.

3. Выводы

Инвариантные системы связи вследствие использования опорных сигналов обладают возможностью защиты передаваемых данных от компроментации. Это обеспечивается маскированием опорных сигналов.

Маскирование может осуществляться разными способами. Наиболее криптостойким из предложенных в статье является способ разделения опорных сигналов на слагаемые с секретными весовыми коэффициентами и секретным расположением слагаемых между информационными сигналами. Дополнительным фактором, обеспечивающим защиту передаваемых данных, является новизна инвариантных методов модуляции.

Таким образом, проведённые исследования показывают перспективность инвариантных систем связи, поскольку они, во-первых, нечувствительны к параметрам каналов связи, а во-вторых, при маскировании опорных сигналов обеспечивают защиту передаваемых данных от компроментации.

Литература

1. Лебедянцев В.В. Разработка и исследование методов анализа и синтеза инвариантных систем связи. Докторская диссертация. СибГУТИ, 1995.
2. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М:Наука, 1974, 832 с.

Статья поступила в редакцию 30.03.2012

Лебедянцев Валерий Васильевич
д.т.н., профессор, заведующий кафедрой автоматической электросвязи СибГУТИ.
Тел(383) 2698242,e-mail: lebvv@mail.sibsutis.ru

Information Security Method in Invariant Communication System

V.V. Lebedyantsev

Information Security Method using reference signal masking is proposed for invariant communication system with block message transfer. Several masking algorithms are described. Cryptographic strength assessment of algorithms is presented.

Keywords: a group of communication channels conversion, channel invariants, invariant communication system, invariant amplitude modulation, reference signal masking, cryptographic strength of masking algorithm.