УДК 004.056.55

АЛГОРИТМ СЛУЧАЙНОГО СЕТЕВОГО КОДИРОВАНИЯ НА ОСНОВЕ РАНГОВЫХ КОДОВЫХ СТРУКТУР

В. В. ПАНЬКОВА

Белорусский государственный университет информатики и радиоэлектроники
(г. Минск, Республика Беларусь)

E-mail: pankova@bsuir.by

Аннотация. В работе рассмотрена модель случайного сетевого кодирования информации на основе ранговых кодовых структур, как компонент комплексного подхода обеспечения безопасности в сетях передачи данных.

Abstract. The paper considers a model of random network coding of information based on rank code structures, as a component of an integrated approach to ensuring security in data transmission networks.

Введение

Важнейшим направлением обеспечения безопасности в сетях передачи данных является использование наиболее приемлемых методов помехоустойчивого кодирования и криптографии. К одному из методов защиты данных принадлежит кодирование информации ранговыми кодами.

Модель сетевого кодирования информации

Моделью сети передачи информации может служить направленный граф. Источник информации из узла S посылает сообщение одновременно m приемникам $R_1,\ldots,R_m$. Максимальное количество информации, переданное от S к R_j, зависит от минимального числа пересечений в графе между S и R_j и часто определяется как проблема широковещательного канала.

Одним из методов достижения максимальной скорости предполагает применение линейного смешивания информации на промежуточных узлах сети по правилу

$$Y = \sum_j a_j X_j,$$

где Y – сигнал на выходе узла., X_j – информационный вектор j-того входа узла, $X_j \in F_q^N$; $\{a_j\}$ – множество весовых коэффициентов кода $a_j \in F_q$.

На вход приемника сети R_j поступает матричный сигнал $\boldsymbol{Y}_j = \boldsymbol{A}_j \boldsymbol{x}$. Строки x, $x_1,\ldots,x_n \in F_q$ определяются информационными пакетами, посланными узлом S. Элементами матрицы $\boldsymbol{A}_j \in F_q^{n\times n}$ являются весовые коэффициенты кода $a_j \in F_q$. Модель сети предполагает, что пакеты могут быть искажены в любом узле сети, при этом сигнал на выходе приемника принимает вид $\boldsymbol{y}_j = \boldsymbol{A}_j \boldsymbol{x} + \boldsymbol{B}_j \boldsymbol{z}$, где $\boldsymbol{B}_j \boldsymbol{z}$ – матрица ошибок.

Определим множество всех подпространств F_q^N как $P(F_q^N)$. Зададим меру расстояния в $P(F_q^N)$ как $\boldsymbol{d_s}(X,Y) = dim(X+Y) - dim\,(X \cap Y)$. Можно задать код подпространства $C \subseteq P(F_q^N)$ с параметрами (N, M, d), если $|C| = M$ и $\boldsymbol{d_s}(U,V) \geq d, \forall U,V \in C$.

Источник S выбирает $V \in C$, находит матрицу $\boldsymbol{x} \in F_q^{n\times N}$, для которой $V\langle \boldsymbol{x} \rangle$, после чего передает $\boldsymbol{x}$. Приемник R_j обрабатывает $U = \langle \boldsymbol{y}_j \rangle \in P(F_q^N)$, причем $U = H_P(V) \oplus I$, где $H_P(V)$ – случайное подпространство V размерности $dim(V)$ - p. Декодер приемника вычисляет оценку V по правилу минимального расстояния

$$V = \arg min_{W\in C} \boldsymbol{d}_s(U,V).$$

Ранговые сетевые коды. Пусть $GF(q)$ – основное (базовое) поле и $GF(q^N)$ – его расширение степени N. Ранговой нормой вектора $(a_1,\ldots,a_n)$, $a_j \in GF(q^N)$, называется максимальное число линейно независимых координат a_j над полем $GF(q)$. Ранговое расстояние между двумя векторами определяется как норма разности двух векторов. Ранговое расстояние линейного кода над полем $GF(q^N)$ определяется как минимальное из всех пар кодовых слов. Расстояние d любого линейного (n, k) – кода удовлетворяет неравенству $d \leq n - k + 1$.

Пусть векторы $g_i \in GF(q^N), i = 1 \dots n, n \le N$ – линейно независимы над полем $GF(q)$ модулярной матрицы G, элементы которой определяются как $g_i^{((l))} = g_i^{jmodN}$. Порождающая матрица кода имеет вид матрицы Вандермонда

$$G_m = \begin{bmatrix} g_1 & g_2 & \cdots & g_n \\ g_1^{((m))} & g_2^{((m))} & \cdots & g_n^{((m))} \\ g_1^{((2m))} & g_2^{((2m))} & \cdots & g_n^{((2m))} \\ \vdots & \vdots & \ddots & \vdots \\ g_1^{(((k-1)m))} & g_2^{(((k-1)m))} & \cdots & g_n^{(((k-1)m))} \end{bmatrix},$$

где $g_i^{((j))} = g_i^{jmodN}$.

Выбрав один раз n линейно независимых векторов над $GF(q^N)$, можем построить $\varphi(N)$ разных порождающих матриц, где $\varphi(N)$ – функция Эйлера.

Криптосистема кодирования. Секретный ключ состоит из 4 частей:

$\boldsymbol{G}$ **–** порождающая матрица рангового кода;

$\boldsymbol{S}$ – строковый скремблер, обратимая $k \times k$ матрица над расширенным полем $GF(q^N)$;

$\boldsymbol{X}$ – шумовая $k \times n$ матрица над расширенным полем с рангами $GF(q^N)$:

- столбцевым рангом t_X над основным полем $GF(q)$,
- рангом r_X над расширенным полем $GF(q^N)$, $r_X \le t_X$;

$\boldsymbol{P}$ – столбцевой скремблер в виде обратимой $n \times n$ матрицы над основным полем $GF(q)$.

Открытым ключом служит матрица $\boldsymbol{G}_{pub} = \boldsymbol{S}(\boldsymbol{X} + \boldsymbol{G})\boldsymbol{P}$.

Открытый текст $m = (m_1 \dots m_k)$ имеет длину k, а его элементы выбираются из поля $GF(q^N)$.

Шифрование

$$\boldsymbol{c} = \boldsymbol{m}\boldsymbol{G}_{pub} + \boldsymbol{e},$$

где $\boldsymbol{e}$ – искусственно добавляемая ошибка рангового веса;

$t_{art\ err} = t - t_X - t_{ch}$ над основным полем $GF(q)$, где t – корректирующая способность рангового кода, t_{ch} – ранговый вес ошибки, исправляемой в канале связи.

Расшифрование

декодер вычисляет $c_s = cP^{-1} = \boldsymbol{m}\boldsymbol{S}(\boldsymbol{X} + \boldsymbol{G}) + \boldsymbol{e}\boldsymbol{P}^{-1}$;

декодирует c_s, результатом является $\boldsymbol{m}_s = \boldsymbol{m}\boldsymbol{S}$;

решает уравнение относительно $\boldsymbol{m}$ и получает исходный текст $\boldsymbol{m}$.

Криптосистема сохраняет корректирующую способность кода.

Заключение

Защита информации требует комплексного подхода. Более высокий уровень защиты данных возможен в каналах с когнитивной связью, за счет работы подслушивающего узла сети в режиме приема на фоне помехи, что приводит к снижению эффективности прослушивания. Дополнительное применение сетевого кодирования информации ранговыми кодами позволит обеспечить в топологии сети области с надежной связью.

Список использованных источников

1. Габидулин Э.М. Теория кодов с максимальным ранговым расстоянием (рус.)// Проблемы передачи информации – 1985. В.1. – Т.21. – С. 3-16.
2. E.M.Gabidulin, N.I. Pilipchuk A new method of erasure correction by rank codes (англ.)// Proceedinds of the 2003 IEEE International Symposium on Information Theory. – Yokohama, Japan: June 29-July 4, 2003/ - C. 423. – ISBN 0-7803-7728-1.
3. Саломатин С.Б., Охрименко А.А. Защита информации в сети передачи информации на основе случайного кодирования ранговыми кодами // Управление информационными ресурсами: материалы VIII международной научно-практической конференции, Минск, 10 февраля 2011 г. / Академия управления при Президенте Республики Беларусь; редкол.: А.В. Ивановский [и др.]. – Минск, 2011. – С. 173-175.