УДК 621.39

ЗАЩИТА ПАКЕТНОЙ СТРУКТУРЫ СЕТЕЙ ПЕРЕДАЧИ ИНФОРМАЦИИ НА ОСНОВЕ КОДА РИДА-СОЛОМОНА

С.Б. САЛОМАТИН, А.А.С. Аль-ЭЗАЙРДЖАВИ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 20 марта 2019

Аннотация. Предложена схема кодовой защиты от потери или повреждения пакетов с помощью кодирования информации кодом Рида-Соломона (РС) в каналах передачи данных. Представлены алгоритмы исправления ошибок и стираний кодом РС.

Ключевые слова: помехоустойчивый код Рида-Соломона, ошибка стирания, широковещательный канал передачи данных

Введение

Одна из угроз нарушения целостности и отказа в обслуживании связана с потерей пакетов в сетях передачи данных и мультимедийной информации. Известные методы защиты от потери или повреждения пакетов данных используют технику автоматического повтора и кодирования данных избыточными корректирующими кодами [1–4].

В работе рассматривается метод защиты от потери или повреждения пакетов с помощью двумерного кодирования информации пространственно-временным кодом РС в широковещательных многоуровневых каналах передачи данных. В основе метода лежит способность кода РС исправлять независимые ошибки и ошибки стирания.

Коды Рида-Соломона

Код РС над полем Галуа $GF(q)$ можно определить как код, состоящий из всех слов $\mathbf{c}=[c_0,c_1,...,c_{n-1}]$ длины n, для которых выполняются $(d-1)$ уравнений [5, 6]:

$$\sum_{i=0}^{n-1} c_i\gamma_i^r = 0 \quad c_i \in GF(q), r_0 \le r \le r_0 + d - 2, \qquad (1)$$

где r_0, и d – произвольные целые числа (не больше n); $\gamma_0,\gamma_1,...,\gamma_{n-1}$ – различные ненулевые элементы конечного поля, которые еще называют локаторами i-й позиций кодового слова. Последовательность локаторов позиций $\{\gamma_i\}$ в (1) произвольна и может быть задана любым удобным способом.

Циклический код РС длины n, равной любому делителю $(q-1)$ задается выражением (1) и последовательностью локаторов положений вида $\gamma_i = \alpha^i$, где α – элемент порядка n в поле $GF(q)$, $\alpha = \sqrt[n]{1}$.

Циклический сдвиг влево на l позиций последовательности $\omega(x)\gamma_i = \alpha^i$ эквивалентен умножению локаторов на α^l: $\gamma_i\alpha^l = \alpha^{i+l \bmod n}$, где $n \mid (q-1)$.

Если некоторый вектор $\mathbf{c}=[c_0,c_1,...,c_{n-1}]$ удовлетворяет (1), то и после сдвига получаем

$$\sum_{i=0}^{n-1} c_i\gamma_i^r\alpha^{l_r} = (\sum_{i=0}^{n-1} c_i\gamma_i^r)\alpha^{l_r} = 0,$$

так как $\alpha^{l_r} \neq 0$ при любых l и r, $r_0 \le r \le r_0 + d$.

Проверочная матрица циклического кода РС имеет вид:

$$H = \left[\alpha^{(r_0+i)\, j \bmod n} \right],\ i = 0, ..., m-1,\ j = 0, ...,\ n-1.$$

Это позволяет рассматривать умножение **H** на вектор **c** как вычисление значений полинома $c(x) = \sum_i c_i x^i$ в точках $\{\alpha^{r_0+i}\}$, $i = 0, 1, ..., m-1$.

Определение синдрома. Предположим, что на вход декодера поступает последовательность символов $(y_0, y_1, ..., y_{n-1})$, где $y_i = c_i + e_i$, $\{e_i\}$ – элементы вектора ошибок, $e_i \in GF(q)$. Синдромом кода называется вектор $\mathbf{s} = (s_0, s_1, ..., s_{d-2})$, элементы которого определяются из выражения

$$s_j = \sum_i y_i \gamma_i^{r_0+j},\ j = 0, 1, ...,\ d-2. \qquad (2)$$

Полином синдрома определяется как

$$s(x) = \sum_{j=0}^{m-1} s_j x^j = \sum_{j=0}^{m-1} x^j \sum_{i=0}^{n-1} e_i \gamma_i^{r_0+j},\ \ m = n-k.$$

Если предположить, что в принятом векторе имеются t ошибок, расположенных на позициях с номерами $i_1, i_2, \ldots, i_t$, то можно записать уравнение

$$s(x)\sigma(x) + x^m \Theta(x) = \omega(x), \qquad (3)$$

где $\sigma(x) = \prod_{v=1}^{t} \left(x\gamma_{i_v} - 1 \right)$, $\omega(x) = -\sum_{v=1}^{t} e_{i_v} \gamma_{i_v}^{r_0} \sum_{\mu=1, \mu \neq v}^{t} \left(x\gamma_{i_\mu} - 1 \right)$; $\Theta(x) = \sum_{v=1}^{t} e_{i_v} \gamma_{i_v}^{r_0+m} \sum_{\mu=1, \mu \neq v}^{t} \left(x\gamma_{i_\mu} - 1 \right)$.

Полином $\sigma(x)$ называют полиномом локаторов ошибок, так как его корни являются обратными величинами локаторов искаженных позиций. Степень $\sigma(x)$ равна t, если число ошибок $t < m$.

Полином $\omega(x)$ называется полиномом значений ошибок (полином ошибок). Степень $\omega(x)$ всегда меньше степени $\sigma(x)$. Полиномы $\sigma(x)$ и $\omega(x)$ взаимно просты.

Уравнение (3) часто используется в виде модульного сравнения, которое называется ключевым уравнением:

$$s(x) \cdot \sigma(x) = \omega(x) \mod x^m. \qquad (4)$$

Если полиномы $\sigma(x)$ и $\omega(x)$ известны, тогда для определения локаторов ошибок достаточно найти корни полинома $\sigma(x)$ среди обратных величин локаторов позиций кода, т. е. найти все решения уравнения $\sigma\left(x^{-1}\right) = 0$, $\sigma(x) x \in \{\gamma_i\}$. Если $\sigma\left(x^{-1}\right)$ имеет степень t и ровно t различных локаторов кода являются его корнями, то можно считать, что в принятом векторе действительно t ошибок. Если же хотя бы один корень $\sigma\left(x^{-1}\right)$ не является локатором кодового слова, то в принятом слове больше, чем $((d-1)/2)$ ошибок и $\sigma(x)$ не является правильным полиномом локаторов ошибок.

Если локаторы ошибок известны, то значения ошибок равны:

$$e_{i_v} = \frac{-\omega\left(\gamma_{i_v}^{-1}\right)}{\gamma_{i_v}^{r_0} \prod_{\mu=1, \mu \neq v}^{t} \left(\gamma_{i_v}^{-1} \gamma_{i_\mu} - 1 \right)}.$$

Выражение значения ошибки можно преобразовать к виду формулы Форни:

$$e_{i_\nu} = \frac{-\omega\left(\gamma_{i_\nu}^{-1}\right)\gamma_{i_\nu}^{-r_0+1}}{\sigma'\left(\gamma_{i_\nu}^{-1}\right)},$$

где $\sigma'(x) = \sum_{\nu=1}^{t} \gamma_{i_\nu} \prod_{\mu=1,\mu\neq\nu}^{t} \left(x\gamma_{i_\mu} - 1\right)$ – формальная производная.

Алгебраический алгоритм декодирования кода РС. Исходные данные: принятое слово $\mathbf{y} = (y_0, y_1, ..., y_{n-1})$; параметры кода – $n,\ k,\ d,\ m = d-1,\ r_0$, локаторы кода – $\gamma_0, \gamma_1, ...$

1. Вычисление синдрома $s(x)$ принятого слова

$$s(x) = \sum_{j=0}^{m-1} s_j x^j, \quad s_j = \sum_{i=0}^{n-1} y_i \gamma_i^{r_0+j}.$$

2. Решение ключевого уравнения $s(x)\cdot\sigma(x) = \omega(x) \mod x^m$. Если степень $\deg(\sigma(x)) \geq m/2$, то отказ и переход к 5.

3. Определение множества локаторов ошибок $Z : z \in Z$, если $\sigma\left(\gamma z^{-1}\right) = 0$. Если же не все корни являются локаторами позиций, то отказ и переход к 5.

4. Вычисление значений ошибок и исправление искаженных позиций $\hat{y}_z = y_z$, если $z \notin Z$, $\hat{y}_z = y_z - e_z$ для $z \in Z$,

$$e_z = \frac{-\omega\left(\gamma_z^{-1}\right)\gamma_z^{-r_0+1}}{\sigma'\left(\gamma_z^{-1}\right)}.$$

5. Восстановление информационных символов или выдача признака отказа от декодирования.

Режим исправления ошибок и стираний. В режиме стирания фиксируются не сами оценки принятых символов, а их местоположение и им присваивается статус стертого символа. Суть исправления и стирания состоит в том, что после декодирования можно провести восстановление стертых символов, используя алгоритмы интерполяции. Если при декодировании использовать l стертых символов, тогда два кода будут отличаться друг от друга по меньшей мере на $(d-l)$ позиций, где d – кодовое расстояние. Тогда в дополнение к стиранию можно будет исправлять $t_m = \lfloor (d-l-1)/2 \rfloor$ ошибок, где $\lfloor x \rfloor$ – это целая часть числа x. Код может исправлять все комбинации из ν ошибок и l стираний в канале, для которого $2\nu + l < d$.

Для восстановления одного стертого символа необходим только один проверочный символ – для восстановления значения, т.к. позиция стирания принимающей стороне известна. Например, для поля Галуа $GF(256)$ код РС (94, 88) из 8-битовых символов имеет n = 94, k = 88 и может исправить до 3 ошибок (t = 3) и восстановить до 6 стертых символов.

Алгоритм исправления стираний. Предположим, что выполнено f стираний при приеме кодового слова, в котором имеется ν ошибок. Обозначим локаторы ошибок как $X_1 = \alpha^{i_1}$, $X_2 = \alpha^{i_2}$, ..., $X_\nu = \alpha^{i_\nu}$, а стираний – как $Y_{c,1} = \alpha^{j_1}$, $Y_{c,2} = \alpha^{j_2}$, ..., $Y_{c,f} = \alpha^{j_f}$. Декодирование ведется в следующем порядке.

1. Вычисляется полином локаторов стираний $\Gamma(x) = \prod_{l=1}^{f} (1 - Y_{c,l} \cdot x)$.

2. В декодируемом векторе заменяются символы с координатами стираний на нулевые символы. Для нового вектора находится полином синдрома стираний $s(x)$.

3. Определяется модифицированный полином синдрома $SE(x) = (\Gamma(x)[1 + s(x)] - 1) \bmod x^{2t+1}$.

4. Вычисляется полином локаторов ошибок $\sigma(x)$ с использованием алгоритма Берлекемпа-Месси и значения модифицированного полинома $SE_i, i = f+1, ..., 2t$.

5. Определяются корни уравнения $\sigma(x)$=0 и координаты ошибок.

6. Составляется ключевое уравнение $\omega(x)=\sigma(x)[1+SE(x)]\bmod x^{2t+1}$ и определяется полином локаторов ошибок-стираний $\psi(x)=\sigma(x)\Gamma(x)$.

7. Оцениваются значения ошибок и стираний. Значения ошибок вычисляются по формуле:

$$Q_{i_k}=\frac{-X_k\omega(X_k^{-1})}{\psi'(X_k^{-1})},$$

где ψ' – формальная производная.

8. Значения стираний вычисляют по формуле: $F_{i_k}=\frac{-Y_k\omega(Y_k^{-1})}{\psi'(Y_k^{-1})}$.

Пример. Декодируется код РС(7, 3) построенный над полем *GF*(8).

Принимаемый вектор равен

$$y(x)=\alpha^4x^6+\alpha^5x^5+\alpha^2x^4+x^3+\alpha^6x^2+\alpha^5x+\alpha^6=y_6x^6+y_5x^5+y_4x^4+y_3x^3+y_2x^2+y_1x+y_0.$$

Приемник выдал стирания на позициях $j_1=1, j_2=6,$ что позволяет записать полином стираний как $er(x)=er_1\ x+er_2\ x^6$.

Алгоритм декодирования.

Вычисляется $\Gamma(x)=(1-\alpha x)\left(1-\alpha^6x\right)=1+\alpha^5x+x^2.$

Символы на 1 и 6 позициях в $y(x)$ заменяются нулями: $y_c(x)=\alpha^5x^5+\alpha^2x^4+x^3+\alpha^6x^2+\alpha^6,$ после чего вычисляется синдром:

$$S_1=y_c(\alpha)=\alpha,\ S_2=y_c\left(\alpha^2\right)=\alpha,\ S_3=y_c\left(\alpha^3\right)=\alpha,\ S_4=y_c\left(\alpha^4\right)=\alpha^3,$$
$$s(x)=\alpha x+\alpha x^2+\alpha x^3+\alpha^3x^4.$$

Модифицируется полином синдрома:

$$SE(x)=\left[\left(1+\alpha^5x+x^2\right)\left(\alpha x+\alpha x^2+\alpha x^3+\alpha^3x^4\right)-1\right]\ \bmod\ x^5=\alpha^6x+\alpha^4x^2+\alpha^6x^3+\alpha^2x^4.$$

С помощью алгоритма Берлекемпа-Месси получается выражение для полинома локаторов ошибок: $\sigma(x)=1+\alpha^3x.$ Локатор ошибки $X_1=\alpha^3.$ Ошибка расположена на третьей позиции.

Ключевое уравнение имеет вид:

$$\omega(x)=\sigma(x)\left[1+SE(x)\right]\bmod x^5=\left(1+\alpha^3x\right)\left(1+\alpha^6x+\alpha^4x^2+\alpha^6x^3+\alpha^2x^4\right)\bmod x^5=1+\alpha^4x+\alpha x^2+\alpha^2x^3.$$

Тогда $\psi(x)=\left(1+\alpha^2x+\alpha^3x^2+\alpha^3x^3\right)$ и формальная производная $\psi'(x)=\left(\alpha^2+\alpha^3x^2\right).$

Вычисляются значения ошибок и стираний:

$$Q_3=\frac{\alpha^3\omega(\alpha^4)}{\psi'(\alpha^4)}=\alpha^6,\ F_1=\frac{\alpha\omega(\alpha^6)}{\psi'(\alpha^6)}=\alpha^5,\ F_6=\frac{\alpha^6\omega(\alpha)}{\psi'(\alpha)}=\alpha^4.$$

Моделирование алгоритма в программной среде MathLab показало эффективность алгоритма в режиме совместного исправления независимых ошибок и стираний

Схема сетевого кодирования

Построим двумерный блок информационных данных размером $K\cdot k,$ где $k=k'm,$ каждые *m* бит представляются как символы конечного поля $GF\left(2^m\right)$. Кодирование осуществляется в два этапа: внешнее кодирование (по столбцам) и внутреннее кодирование (по строкам).

Внешнее кодирование осуществляется кодом РС над полем $GF\left(2^m\right)$. Каждому столбцу ставится в соответствие кодовое слово $C_1(n_1, K),$ где $n_1=K+r_0,$ r_0 – число избыточных

символов. Блок содержит k' кодовых слов. Каждая строка блока дополняется заголовком из s бит, после чего кодируется внутренним кодом $C_2(n_2, k_2)$. Каждой строке блока ставится в соответствие код, имеющий, r_2 избыточных бит и длину $n = n_2 = s + k + r_2$, где $k = k_2 - s$. Схема формирует K информационных и r_0 избыточных пакетов в блоке.

Система многоуровневого кодирования. Выберем из каждого пакета информации K' символов $(m \times K')$ бит. Рассматривая эти символы как информационные, можно выполнить кодирование внешним кодом. Аналогичным образом следует поступить с K' избыточными символами каждого внешнего кодового слова.

Предположим, что система имеет L уровней, и на каждом i-ом уровне имеются K_i информационных и R_i избыточных пакетов. В схеме защиты выполняются следующие соотношения: $0 \le K_1 \le K_2 \le ... \le K_L$ и $R_1 \ge R_2 \ge ... \ge R_L \ge 0$.

Если длина блока равна $n_i = K_i + R_i$, то система защиты должна использовать базовый код $\mathrm{PC}(n, k)$, параметры которого должны удовлетворять неравенствам: $n \ge \max\limits_{\forall i}\{n_i\}$ и $k \ge \max\limits_{\forall i}\{K_i\}$, $(n-k) \ge \max\limits_{\forall i}\{R_i\}$.

Структура базового кода должна быть согласована со структурами кодов $\mathrm{PC}(n_i, K_i)$.

Пример. Пусть в блоке передаются 48 информационных пакетов и 12 избыточных пакетов. Выберем по 4 байта из каждого информационного пакета и закодируем 192 байта кодом РС (240, 192). Выберем 4 символа из числа избыточных в каждом полученном коде и используем их в качестве избыточных символов для исправления пакетных ошибок. Таким образом, может быть сформирован пакет из 256 кодов слов кода РС.

Заключение

Корректирующая способность схемы защиты зависит от минимальных кодовых расстояний кодов. Пусть d минимальное кодовое расстояние, ν число ошибок и μ число стираний в принятом слове. Тогда выбор d определяется неравенством $d \ge 2\nu + \mu$. Система кодирования может осуществлять дополнительную функцию распределения ключей, учитывая возможности использования кода РС в полилинейных схемах распределения.

PROTECTION OF THE PACKET STRUCTURE OF INFORMATION TRANSMISSION NETWORKS BASED ON REED-SOLOMON CODE

S.B. SALOMATIN, A.A.S. Al EZAYRDJAVI

Abstract. A code protection scheme against packet loss or damage using the Reed-Solomon code (RS) in data transmission channels is proposed. Algorithms for error correction and erasure by the RS code are given.

Keywords: error-proof Reed-Solomon code, erasure error, broadcast data channel.

Список литературы

1. Rizzo L. // ACM Computer Communication Review. 1997. Vol. 27. No. 2. P. 24–36.
2. Xu. Y., Zhang. T. // IEEE Trans on Broadcasting. 2002. Vol. 48. No. 3. P. 237–245
3. Luby M.G. [et. al.] // Information Theory, IEEE Transactions on. 2001. Vol. 47(2). P. 569–584.
4. Guang X., Fu F.W., Zhang Z. // International Symposium on Network Coding, NetCod. 2011. P. 1–6.
5. Мак-Вильямс Ф.Дж., Слоэн Н.Дж.А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
6. Влэдуц С.Г., Ногин Д.Ю., Цфасман М.А. Алгеброгеометрические коды. Основные понятия. М.: МЦНМО, 2003.