Семеренко В. П., к.т.н., доцент, кафедра вычислительной техники,
Винницкий национальный технический университет, Украина

Защита информации в многоканальных системах связи

Вступление. Теоретические основы передачи данных и их защиты были заложены известным американским ученым К. Шенноном еще в середине прошлого века [1]. Разработанные с тех пор помехоустойчивые коды и криптографические алгоритмы ориентированы в основном на единственный канал связи.

Однако, передача данных может быть организована одновременно от P передатчиков к P приемникам по P параллельным каналам. Такая ситуация типична для цифрового радиовещания и телевидения, оптоволоконных систем связи, компьютерных сетей и других [2, с. 126], [3].

P-канальная система передачи данных не является простым соединением P отдельных каналов. Для многоканальной системы характерна иная модель ошибок, а также свои особенности архитектуры. Поэтому актуальной является разработка новых подходов в организации защиты данных, которые максимально учитывают специфику многоканальной связи.

Могут быть различные причины возникновения нарушений в передаваемых данных: либо вследствие ошибок, обусловленных естественными явлениями в линиях связи, либо из-за преднамеренно введенных искажений, либо же вследствие неисправности радиоэлектронной аппаратуры. С целью экономии времени желательно совместить проверку нарушений данных разного происхождения [4].

Цель исследований – разработать теоретические основы интегрованной защиты данных для многоканальной связи на основе теории циклических кодов и математического аппарата линейных последовательностных схем (ЛПС).

Математические основы защиты данных для многоканальной связи. Введем автоматную модель циклических кодов над полем Галуа $GF(2)$ на основе теории ЛПС [5, с. 46].

Пусть имеется традиционный циклический (n, k)-код Ω, заданный порождающим полиномом

$$g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_{r-2} x^{r-2} + g_{r-1} x^{r-1}. \qquad (1)$$

Традиционная ЛПС Λ с одним входом, одним выходом и r элементами памяти в дискретные моменты времени t над полем Галуа $GF(2)$ задается функцией состояний (переходов)

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2), \tag{2}$$

и функцией выходов

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2), \tag{3}$$

где $A = \lfloor a_{ij} \rfloor_{r \times r}$, $B = \lfloor b_{ij} \rfloor_{r \times 1}$, $C = \lfloor c_{ij} \rfloor_{1 \times r}$, $D = \lfloor d_{ij} \rfloor_{1 \times 1}$ – характеристические матрицы; $S(t) = [s_i]_r$, $U(t) = [u_i]_1$, $Y(t) = [y_i]_1$ – соответственно, слова состояния, входное и выходное.

Размерности матриц ЛПС Λ и параметры циклического кода Ω связаны через коэффициент r, который для кода равен числу контрольных разрядов кодового вектора Z при систематическом кодировании ($r = n - k$).

Для помехоустойчивого кодирования в ρ-канальной связи может использоваться параллельный циклический (n, k, ρ)-код $\Omega_{(\rho)}$ [6], наиболее пригодной математической моделью которого является ρ-канальная ЛПС ($\rho \le (n-k)$). Такую ЛПС можно получить из вышеописанной одноканальной ЛПС Λ, которую назовем порождающей.

ОПРЕДЕЛЕНИЕ 1. ρ-канальная ЛПС $\Lambda_{(\rho)}$ над полем Галуа $GF(2)$ – это конечный автомат линейного типа (линейный автомат) с r элементами памяти, ρ входами и ρ выходами, который в дискретные моменты времени t задается функцией состояний (переходов)

$$S(t+1) = A_{(\rho)} \times S(t) + B_{(\rho)} \times U_{(\rho)}(t), \qquad GF(2) \tag{4}$$

и функцией выходов

$$Y_{(\rho)}(t) = C_{(\rho)} \times S(t) + D_{(\rho)} \times U_{(\rho)}(t), \qquad GF(2), \tag{5}$$

где $A = \lfloor a_{ij} \rfloor_{r \times r}$, $B = \lfloor b_{ij} \rfloor_{r \times \rho}$, $C = \lfloor c_{ij} \rfloor_{\rho \times r}$, $D = \lfloor d_{ij} \rfloor_{\rho \times 1}$ – характеристические матрицы; $S(t) = [s_i]_r$, $U(t) = [u_i]_\rho$, $Y(t) = [y_i]_\rho$ – соответственно, слова состояния, входное и выходное.

Основная характеристическая матрица $A_{(\rho)}$ ρ-канальной ЛПС $\Lambda_{(\rho)}$ полностью совпадает с основной характеристической матрицей A порождающей одноканальной ЛПС Λ. При $\rho = r$ матрицы A и $A_{(\rho)}$ могут быть следующими:

$$A_{(\rho)} = A = \begin{vmatrix} 0 & 0 & 0 & \dots & g_0 \\ 1 & 0 & 0 & \dots & g_1 \\ 0 & 1 & 0 & \dots & g_2 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 1 & g_{r-1} \end{vmatrix}. \quad (6)$$

Элементы последнего столбца матрицы (6) представляют собой коэффициенты полинома (1), т. е. код $\Omega_{(\rho)}$ основан на том же порождающем полиноме, что и циклический код Ω.

Каждый такт времени на ρ входов ЛПС $\Lambda_{(\rho)}$ поступает ρ-разрядное входное слово $U_{(\rho)}(t)$, а с ее выходах формируется ρ-разрядное выходное слово $Y_{(\rho)}(t)$. Таким образом, параллельный циклический (n, k, ρ)-код $\Omega_{(\rho)}$ над полем $GF(2)$ можно рассматривать как циклический код, состоящий из ρ кодовых слов Z_i $(i = 1 \dots \rho)$, объединенных в кодовую матрицу:

$$Z_{(\rho)} = \begin{bmatrix} z_1 \\ z_2 \\ \dots \\ z_\rho \end{bmatrix} = \begin{bmatrix} z_{11} & z_{12} & \dots & z_{1n} \\ z_{21} & z_{22} & \dots & z_{2n} \\ \dots & \dots & \dots & \dots \\ z_{\rho 1} & z_{\rho 2} & \dots & z_{\rho n} \end{bmatrix}, \quad GF(2), \quad (7)$$

Защита данных на основе помехоустойчивого кодирования и криптографии. В различных системах передачи данных широко используется циклический избыточный контроль (*Cyclic Redundancy Check – CRC*) [7, с. 247]. Напомним, что суть метода заключается в вычислении контрольной суммы Σ, которая позволяет определять возможные искажения в проверяемой входной последовательности данных.

Рассмотрим интерпретацию операции декодирования циклических кодов на основе их автоматной модели. При подаче на входы кодовой матрицы (7) ЛПС $\Lambda_{(\rho)}$ через n тактов времени из начального нулевого состояния $S(0)$ согласно (2) перейдет в некоторое состояние $S(n)$, называемое синдромом.

В многоканальной системе произвольная входная последовательность данных представляет собой некоторую $(\rho \times n)$-матрицу $I_{(\rho)}$. Если выполнить рекурсивные вычисления

$$S(t+1) = A_{(\rho)} \times S(t) + B_{(\rho)} \times I_{(\rho)}(t), \quad GF(2), \quad (8)$$

тогда полученный синдром $S(n)$ будет представлять собой контрольную сумму Σ, а ненулевое значение $S(n) \neq S(0)$ будет свидетельствовать о наличии ошибки в $I_{(\rho)}$.

В криптографии для проверки целостности данных используется поточное хеширование, в результате которого длинная информационная ($\rho \times n$)-матрица $I_{(\rho)}$ преобразуется в хеш-функцию $H(X)$ заданной длины [8]. Процедуру хеширования очень просто осуществить, используя аппарат ЛПС: хеш-функция $H(X)$ совпадает со значением синдрома $S(n)$, в которое перейдет ЛПС под воздействием ($\rho \times n$)-матрицы $I_{(\rho)}$ согласно (8).

Таким образом, можно утверждать, что циклический избыточный контроль и поточная хеш-функция $H(X)$ – это разные наименования результата одних и тех же математических действий. Одновременно следует отметить, что преобразование (8) будет уязвимым как с позиций помехоустойчивого кодирования, так и с позиций криптографии, поскольку обе задачи имеют разные критерии эффективности полученного решения.

Помехоустойчивый код должен обнаруживать максимальное количество ошибок. Поэтому для усиления корректирующих способностей CRC-кода (возможности обнаружения всех двойных случайных ошибок и пакетов ошибок) необходимо ввести дополнительный контроль строк по четности и выбирать его порождающий полином (1) как разложимый вида

$$g(x) = (1+x)\,p(x), \qquad (9)$$

где $p(x)$ – примитивный полином.

С другой стороны, важнейшим свойством хэш-функции является ее односторонность. В [9] доказано, что односторонность функции связана с существованием криптостойких псевдослучайных генераторов. ЛПС, которая реализует преобразование (6), будет являться генератором псевдослучайных чисел максимального периода $2^n - 1$, если соответствующий ей порождающий многочлен (1) будет примитивным. При выборе полинома вида (9) период псевдослучайной последовательности уменьшится вдвое.

Более существенным является то, что CRC-коды непригодны при умышленном искажении информации, поскольку злоумышленник может легко видоизменить исходное сообщение без изменения самой контрольной суммы. Однако, можно повысить криптостойкость контрольной суммы, а значит, и поточной хэш-функции, следующими мерами.

Рассмотрим защиту от подмены исходных данных противником, которому известны значение $H(X)$ и характеристические матрицы $A_{(\rho)}$ и $B_{(\rho)}$ ЛПС $\Lambda_{(\rho)}$. Из исходного нулевого состояния $S(0)$ ЛПС $\Lambda_{(\rho)}$ под воздействием секретного ключа К1 (($\rho \times r$)-матрицы) переводится в состояние $S(r)$, затем под воздействием основной информационной ($\rho \times n$)-матрицы $I_{(\rho)}$ – в состояние $S(n+r)$ и, в завершение, под воздействием секретного ключа К2 ((

$\rho \times r$)-матрицы) – в конечное состояние $S(n+2r)$, которое и объявляется защищенной потоковой хэш-функцией $H(X)$ (рис. 1).

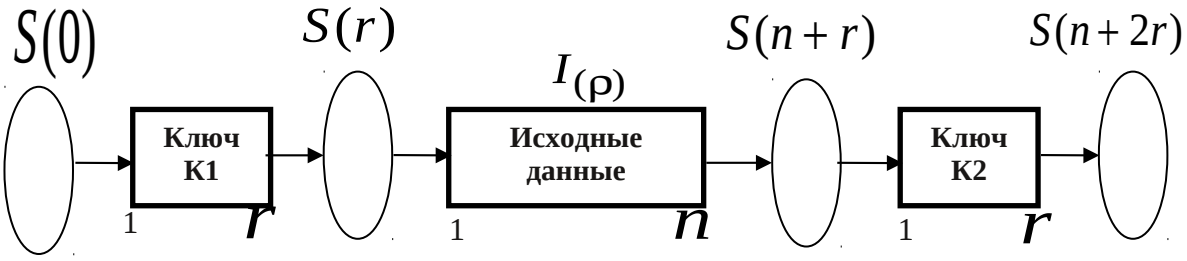

Рисунок 1 – Формирование защищенной хэш-функции

Выводы. Помехоустойчивое кодирование в системах передачи данных и хеширование данных в криптографии направлены на решение одной задачи – задачи проверки целостности данных. Эти две разновидности преобразования информации дополняют друг друга, а их совместное использование позволяет эффективно использовать каналы связи для надежной защиты передаваемой информации. На основе общего математического аппарата – теории ЛПС – можно получить проверочную функцию, которую можно рассматривать и как контрольную сумму CRC и как потоковую хэш-функцию. Для учета специфики обеих способов контроля необходимо использовать компромиссные решения, что позволит совместить во времени операции кодирования и криптозащиты и достичь максимального результата проверки. Особую актуальность это имеет в современных многоканальных системах передачи данных.

Литература

1. Шеннон К. Работы по теории информации и кибернетике / К. Шеннон – М. : Изд-во иностр. лит., 1963. – 829 с.
2. Габидулин Э. М. Кодирование в радиоэлектронике / Э. М. Габидулин, В. Б. Афанасьев – М.: Радио и связь, 1986. – 176 с.
3. Слепов Н. Н. Современные технологии цифровых оптоволоконных сетей связи / Н. Н. Слепов. – Изд. 2-е, испр. – М. : Радио и связь, 2003. – 468 с.
4. Семеренко В. П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование / В. П. Семеренко // Захист інформації, 2011. – № 3. – С. 44–52.
5. Гилл А. Линейные последовательностные машины / А. Гилл ; пер. с англ. – М. : Наука, 1974. – 288 с.
6. Семеренко В. П. Паралельні циклічні коди / В. П. Семеренко // Вісник ВПІ. – 2014. – № 6. – С. 65–72.
7. Столлингс В. Компьютерные системы передачи данных / В. Столингс. ; Изд. 6-е; пер. с англ. – М., Издательский дом «Вильямс», 2002. – 928 с.
8. Семеренко В. П. Разработка хэш-функции на основе поточного шифрования / В. П. Семеренко, П. В. Ширшова // Защита информации : сборник научных трудов НАУ, Вып. 15. – К. : НАУ, 2008. – С.163–166.
9. Impagliazzo R. Pseudo-random generation from one-way functions / R. Impagliazzo, L. Levin, M. Luby // Proc. 21st Annu. ACM Symp. on Theory of Computing. – 1989. – P. 12–24.