УДК 004.056

В.П. Цветов

Самарский национальный исследовательский университет имени академика С.П. Королева

О МАТРИЧНОЙ МОДЕЛИ МУЛЬТИПЛЕКСИРОВАНИЯ ЦИФРОВЫХ ПОТОКОВ

В работе рассматривается матричная модель мультиплексирования потоков двоичных данных, позволяющая наглядно представить структуру агрегатного потока и определить его емкостные характеристики. Модель пригодна для описания скремблирования цифровых потоков с целью защиты передаваемой информации.

Ключевые слова: телекоммуникационные системы, математическое моделирование, защита данных.

Введение

Цифровые информационно-телекоммуникационные системы в настоящее время являются главными составляющими глобального информационного пространства. Имеется большое количество работ, посвященных обеспечению безопасности телекоммуникационных средств, в т.ч. относящихся к области образования и организации учебного процесса [1-4]. Параметры цифровых сигналов описываются конечным множеством возможных значений функций дискретного времени и, поэтому, допускают представление средствами дискретных моделей. Одна из таких моделей будет рассмотрена ниже.

2. Матричная модель мультиплексирования

Рассмотрим многоканальную цифровую телекоммуникационную систему (ЦТС) с m компонентными потоками $s_k, k \in 1..m$ и агрегатным потоком a, передаваемым по каналу связи с пропускной способностью n бит/Δt. Будем обозначать скорость передачи данных в потоке s_k, как n_k бит/Δt. Понятно, что $\sum_{k=1}^{m} n_k = n_0 \le n$. Представим дискретное состояние агрегатного потока в

промежутке времени $[t, t+\Delta t]$ при помощи строки (a_j) длины n, в которой на j-ом месте стоит значение бита, переданного в течение длительности интервала импульса $\left[t, t+\frac{\Delta t}{n} j\right]$ агрегатного потока.

Аналогичным образом, представим дискретное состояние каждого из компонентных потоков при помощи строк $(s_i^k) = (s_1^k, .., s_{n_k}^k)$ длины n_k. Для этого будем считать, что в строке (s_i^k) на i-ом месте стоит значение бита, принятого на вход запоминающего устройства, предназначенного для считывания данных из компонентного потока s_k, в порядке поступления этого бита на вход в течение промежутка времени $[t, t+\Delta t]$.

Образуем *композитную строку* (S_i) длины $n_0 = \sum_{k=1}^{m} n_k$, последовательно записывая в нее элементы строк (s_i^k), т.е. полагая:

$$(S_i) = (s_1^1, .., s_{n_1}^1, s_1^2, .., s_{n_2}^2, .., s_1^m, .., s_{n_m}^m)$$

Определим инъекцию $F : 1..n_0 \to 1..n$, считая значением $F(i)$ номер позиции переданного бита S_i в представлении агрегатного потока (a_j).

Определим прямоугольную *агрегирующую матрицу* (M_{ij}) размерности $n_0 \times n$, считая все ее элементы равными нулю, за исключением элементов $M_{iF(i)} = 1$. По построению, в каждой строке этой матрицы стоит ровно одна единица, а в каждом столбце – не более одной единицы, при этом нулевой столбец соответствует биту агрегатного потока, не занятого под передачу данных компонентных потоков. Нулевые столбцы будут отсутствовать в матрице (M_{ij}) только в случае $n_0 = n$, таком образом, отношение $\frac{n_0}{n}$ можно рассматривать как меру загруженности агрегатного потока.

Матрица (M_{ij}) совместно с набором скоростей $(n_k) = (n_1, .., n_m)$ определяет схему мультиплексирования с точностью до свободных битов агрегатно-

го потока, которые обычно занимаются под передачу служебной информации, в т.ч. синхронизирующего сигнала.

Таким образом, пару $\left\langle \left(M_{ij}\right),\left(n_k\right)\right\rangle$ можно рассматривать как модель мультиплексирования ЦТС.

В силу построения, должны выполняться равенства

$$\left(M_{ij}\right)\circ\left(M_{ij}\right)^T=\left(\sum_{k=1}^{n}M_{ik}\cdot M_{jk}\right)=\left(\delta_{ij}^{n_0}\right),$$

$$\left(M_{ij}\right)^T\circ\left(M_{ij}\right)=\left(\sum_{k=1}^{n_0}M_{ki}\cdot M_{kj}\right)=\left(\delta_{ij}^{n}\right),$$

$$\left(a_j\right)=\left(S_i\right)\circ\left(M_{ij}\right)=\left(\sum_{i=1}^{n_0}S_i\cdot M_{ij}\right),$$

$$\left(S_i\right)=\left(a_j\right)\circ\left(M_{ij}\right)^T=\left(\sum_{j=1}^{n}a_j\cdot M_{ji}\right).$$

где через $\left(\delta_{ij}^{n}\right)$ обозначена единичная матрица порядка n.

Кроме того, если обозначить $\left(N_i\right)=\left(1,2,..,n_0\right)$, то

$$\left(F^{-1}(j)\right)=\left(N_i\right)\circ\left(M_{ij}\right)=\left(\sum_{i=1}^{n_0}N_i\cdot M_{ij}\right),$$

где $\left(F^{-1}(j)\right)$ обозначает *порядковую строку*, все элементы которой равны нулю, за исключением элементов $F^{-1}\left(F\left(i\right)\right)=i$. Порядковая строка фиксирует появление номеров битов композитной строки в представлении агрегатного потока.

В качестве примера рассмотрим модель $\left\langle \left(M_{ij}\right),\left(n_k\right)\right\rangle$ для схемы мультиплексирования двух компонентных потоков s_1 и s_2, имеющих одинаковые скорости $n_1=n_2=2$ бит/Δt в агрегатный поток a, который передается по 238ннналу связи с пропускной способностью 8 бит/Δt. Пусть схема мультиплексирования определяется агрегирующей матрицей

$$\left(M_{ij}\right)=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&1&0&0\end{pmatrix}$$

Тогда для дискретных представлений компонентных потоков $\left(s_i^1\right)=\left(s_i^2\right)=(1,1)$ получаем композитную строку $\left(S_i\right)=(1,1,1,1)$, а также представление агрегатного потока и порядковой строки в виде: $\left(a_j\right)=\left(S_i\right)\circ\left(M_{ij}\right)=(1,1,0,0,1,1,0,0)$, $\left(F^{-1}(j)\right)=\left(N_i\right)\circ\left(M_{ij}\right)=(1,3,0,0,2,4,0,0)$

Предложенную схему можно естественным образом детализировать, добавив в рассмотрение $\tilde{m}$ компонентных потоков служебных данных $\tilde{s}_l$ со скоростями $\tilde{n}_l$, а также псевдопоток свободных битов $\overline{s}_0$ со скоростью $\overline{n}_0$ так, чтобы обеспечить выполнение равенства $\sum_{k=1}^{m}n_k+\sum_{l=1}^{\tilde{m}}\tilde{n}_l+\overline{n}_0=n$. При этом все элементы строк агрегирующей матрицы $\left(M_{ij}\right)$, соответствующие псведопотоку свободных битов, считаем равными нулю.

В контексте предыдущего примера можно использовать четвертый и восьмой биты агрегатного потока для передачи служебных данных со скоростью 2 бит/Δt, обозначив его представление $\left(\tilde{s}_i^3\right)=\left(\tilde{s}_1^3,\tilde{s}_2^3\right)$. В этом случае квадратная *обобщенная агрегирующая матрица* $\left(M_{ij}\right)$ порядка $n=8$ будет иметь вид

$$\left(M_{ij}\right)=\begin{pmatrix}1&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0\\0&1&0&0&0&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&0&0\\0&0&0&0&0&0&0&0\end{pmatrix}$$

Соответственно, $\left(F^{-1}(j)\right)=\left(N_i\right)\circ\left(M_{ij}\right)=(1,3,0,5,2,4,0,6)$.

Вообще говоря, любая матрица $\left(M_{ij}\right)$ порядка n, в каждой строке и 240нждом столбце которой стоит не более одной единицы, может рассматриваться как обобщенная агрегирующая матрица некоторой ЦТС. Более того, любая матрица, полученная из агрегирующей перестановкой ее строк и/или столбцов, при сохранении нумерации элементов композитной строки может быть интерпретирована как схема скремблирования агрегатного потока данной ЦТС.

Различные схемы скремблирования $\left(M_{ij}\right)^s$ будут получаться при помощи матрицы $\left(M_{ij}\right)$ и пары квадратных матриц перестановок $\left(P_{ij}^1\right)$ и $\left(P_{ij}^2\right)$ из соотношения

$$\left(M_{ij}\right)^s = \left(P_{ij}^1\right) \circ \left(M_{ij}\right) \circ \left(P_{ij}^2\right) = \left(\sum_{k=1}^{n} P_{ik_1}^1 \cdot M_{k_1 k_2} \cdot P_{k_2 j}^2 \right).$$

Напомним, что матрицами перестановок называют квадратные матрицы порядка n, в каждой строке и каждом столбце которых стоит ровно одна единица.

В итоге, четверку $\left\langle \left(M_{ij}\right), \left(P_{ij}^1\right), \left(P_{ij}^2\right) \left(n_k\right) \right\rangle$ можно интерпретировать как модель защиты данных в ЦТС.

Литература

1. Белов Е.Б., Лось В.П., Проскурин В.Г., Черемушкин А.В. О проекте профессионального стандарта «Специалист по безопасности компьютерных систем и сетей» // Информационное противодействие угрозам терроризма, 2015, т. 3, № 25, с. 18-21.

2. Белов Е.Б., Потапченко М.А., Шалимов И.А. Материально техническое обеспечение сетевых дисциплин по специальности «Информационная безопасность телекоммуникационных систем» // Информационное противодействие угрозам терроризма, 2015, т. 1, № 25, с. 56-62.

3. Осипов М.Н. Концепция разработки лабораторного практикума по защите информации коллективного пользования на основе среды программирования Labview // Информационное противодействие угрозам терроризма, 2015, т. 1, № 25, с. 317-320.

4. Крыжановский А.В., Кухарев С.Н., Афанасьев В.Н. Реализация лабораторного практикума дисциплины «Информационная безопасность телекоммуникационных систем» специальности 10.05.02 // Информационное противодействие угрозам терроризма, 2015, т. 1, № 25, с. 224-234.