# ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ И СЖАТИЯ ИНФОРМАЦИИ

DOI 10.17223/20710410/26/7

УДК 517.19

## ОЦЕНКА СТОЙКОСТИ КОДОВОГО ЗАШУМЛЕНИЯ К $l$-КРАТНОМУ ЧАСТИЧНОМУ НАБЛЮДЕНИЮ В СЕТИ

И. И. Винничук, Ю. В. Косолапов

*Южный федеральный университет, г. Ростов-на-Дону, Россия*

**E-mail:** ilonavinnichuk144@gmail.com

Рассматривается сеть передачи данных с линейным кодированием в узлах. Предполагается, что наблюдатель подслушивает данные, передаваемые по некоторым рёбрам сети, а информация, поступающая на вход сети, защищается с помощью кодового зашумления. В рамках этой модели решается задача анализа стойкости кодового зашумления при многократном подслушивании в сети данных, соответствующих одному информационному слову. Получена формула вычисления стойкости после $l$ перехватов для $l \geqslant 1$. Для одной сети в качестве примера рассмотрено применение полученной формулы при анализе стойкости кодового зашумления, основанного на коде Рида — Маллера $\mathcal{R}(1,3)$.

**Ключевые слова:** *сетевое кодирование, частичное наблюдение, кодовое зашумление, анализ стойкости.*

### Введение

В работе рассматривается передача данных по сети связи, в узлах которой над принятыми данными выполняются линейные операции. Такие сети отличаются от традиционных сетей, где узлы могут только принимать, временно хранить и передавать данные другим узлам [1]. В работах [2–4] показано, что с помощью методов сетевого кодирования можно увеличить пропускную способность сети. В частности, в [4] показано, как повысить производительность сети без радикальных изменений в инфраструктуре сети передачи данных. Отметим, что пропускная способность сети может быть увеличена в случае, когда получателей не менее двух.

Как и в случае каналов связи, в сетях связи также возникает задача защиты конфиденциальности передаваемых данных от несанкционированного ознакомления (наблюдения). Кроме естественных методов защиты, основанных на применении криптографических преобразований, в последнее время активно исследуются методы, специфичные для сетей [5, 6]. Эти методы основаны на том, что потенциальному наблюдателю доступны не все передаваемые по сети данные, а только их часть. Такой подход оправдан по той причине, что сеть, как правило, географически распределена и контролирование всех каналов сети для наблюдателя в большинстве случаев может оказаться неприемлемым или невозможным. Учитывая частичную доступность данных наблюдателю, одним из подходящих способов защиты является метод кодового зашумления, использованный в [7] для защиты данных от частичного наблюдения в канале.

По частично наблюдаемым данным подслушивающий может построить множество возможных информационных блоков (претендентов), которым соответствуют наблюдаемые данные. Чем больше мощность этого множества претендентов, тем больше неопределённость наблюдателя относительного информационного блока и соответственно тем лучше защита. Часто, в силу особенности структуры, передаваемое сообщение (состоящее из набора информационных блоков) содержит повторяющиеся блоки. Эта особенность даёт возможность наблюдателю провести атаку многократного подслушивания с целью уменьшить мощность множества претендентов. В частности, наблюдатель может провести атаку многократного частичного подслушивания в сети. В случае применения метода кодового зашумления задача наблюдателя по сокращению множества претендентов усложняется за счёт того, что одному информационному блоку, в силу особенностей метода, соответствуют разные кодовые блоки.

Модель многократного частичного подслушивания в канале рассмотрена, например, в [8], где получена зависимость неопределённости наблюдателя от множеств наблюдаемых координат, когда данные перед отправкой в канал преобразуются с помощью метода кодового зашумления. В настоящей работе ставится задача оценки неопределённости наблюдателя в рамках модели многократного наблюдения частичных данных в сети с линейными преобразованиями в узлах, когда информационные блоки на входе сети кодируются с помощью метода кодового зашумления.

Работа организована следующим образом. В п. 1.1 и 1.2 приведены необходимые сведения о линейном сетевом кодировании и методе кодового зашумления соответственно. В п. 1.3 строится модель многократного перехвата в сети и вводится мера неопределённости наблюдателя после многократного перехвата. Оценке этой меры посвящён п. 2, где в п. 2.1 эта мера оценивается в случае однократного перехвата, а в п. 2.2 этот результат обобщается на случай многократного перехвата. В п. 2.3 приводится пример вычисления меры неопределённости для одной сети и кода Рида — Маллера $\mathcal{R}(1,3)$.

## 1. Предварительные сведения и результаты

### 1.1. Сетевое кодирование

Приведём необходимые сведения из теории сетевого кодирования. Пусть $\mathbb{F}_q$ — конечное поле. Сеть связи $\mathcal{N}$, состоящая из одного источника $S$, $t$ получателей и промежуточных узлов, представляется в виде конечного связанного направленного графа. Стоит отметить, что для повышения пропускной способности сети необходимо выполнение условия $t \geqslant 2$ [2], однако результат, полученный в настоящей работе, может быть применён и для сетей, где $t = 1$. Поэтому здесь и далее с целью общности полагается, что $t$ — произвольное натуральное число. Множества всех узлов и рёбер сети $\mathcal{N}$ обозначим соответственно $\mathcal{V}$ и $\mathcal{E}$; $v(\mathcal{N}) = |\mathcal{V}|$, $e(\mathcal{N}) = |\mathcal{E}|$. Узлы сети будем обозначать прописными латинскими буквами, а рёбра — строчными. Для узла $U$ множества входных и выходных рёбер обозначим $\mathrm{In}(U)$ и $\mathrm{Out}(U)$ соответственно. Будем полагать, что источник $S$ имеет $n$ мнимых входных ребер, множество которых обозначим $\mathrm{Im}(S)$, $|\mathrm{Im}(S)| = n$, и по мнимым входным рёбрам в источник $S$ загружается вектор данных $\mathbf{x} \in \mathbb{F}_q^n$, который необходимо передать по сети: по каждому мнимому ребру загружается одна компонента вектора $\mathbf{x}$. Предполагается, что в сети $\mathcal{N}$ нет помех.

Линейный сетевой код размерности $n$ задается с помощью линейных локального и глобального кодирующих отображений, а именно: для узла $U$ и канала $e \in \mathrm{Out}(U)$ локальным кодирующим отображением называется отображение вида $\widetilde{k}_e : \mathbb{F}_q^{|\mathrm{In}(U)|} \to \mathbb{F}_q$, а глобальным кодирующим отображением для узла $U \neq S$ и канала $e \in \mathrm{Out}(U)$ — отображение вида

$$\widetilde{f}_e : \mathbb{F}_q^n \to \mathbb{F}_q,$$

однозначно определяемое с помощью упорядоченного множества $\{\widetilde{f}_d(x)) : d \in \mathrm{In}(U)\}$ и локального отображения $\widetilde{k}_e$ для этого ребра $e$ [9]. Так как сеть линейная, для узла $U$ каждому локальному отображению $\widetilde{k}_e$, $e \in \mathrm{Out}(U)$, можно сопоставить вектор-столбец $\widetilde{\mathbf{k}}_e \in \mathbb{F}_q^{|\mathrm{In}(U)|}$, определяющий это отображение. Тогда узлу $U$ соответствует $(|\mathrm{In}(U)| \times |\mathrm{Out}(U)|)$-матрица локальных сетевых линейных преобразований, составленная из столбцов $\widetilde{\mathbf{k}}_e$:

$$K_U = [\widetilde{\mathbf{k}}_e]_{e\in \mathrm{Out}(U)}. \tag{1}$$

Матрица (1) для $U$ позволяет по значениям на входных рёбрах узла $U$ вычислить значения на его выходных рёбрах. Линейному отображению $\widetilde{f}_e$ также можно однозначно сопоставить вектор-столбец $\widetilde{\mathbf{f}}_e \in \mathbb{F}_q^n$ высоты $n$, определяющий это отображение:

$$\widetilde{\mathbf{f}}_e = [f_{e,1}, \ldots, f_{e,n}]^{\mathrm{T}}, \tag{2}$$

где символом $\mathbf{a}^{\mathrm{T}}$ обозначаем транспонирование вектора $\mathbf{a}$. Отметим, что для источника $S$ набор $(\widetilde{\mathbf{f}}_e)_{e\in \mathrm{Im}(S)}$ должен образовывать базис векторного пространства $\mathbb{F}_q^n$. Глобальное отображение $\widetilde{f}_e$ позволяет по вектору входных данных длины $n$ определить элемент поля $\mathbb{F}_q$, передаваемый по ребру $e$. Другими словами, по известному входному вектору $\mathbf{x}$, загружаемому по мнимым рёбрам в источник $S$ сети $\mathcal{N}$, для каждого ребра $e \in \mathcal{E}$ можно определить передаваемое по этому ребру значение, используя глобальное отображение (2) для этого ребра. Таким образом, по вектору $\mathbf{x}$ можно построить вектор значений, передаваемых по рёбрам сети $\mathcal{N}$, вида

$$\mathcal{F}(\mathbf{x}) = (\widetilde{f}_e(\mathbf{x}))_{e\in\mathcal{E}}. \tag{3}$$

Отметим, что координаты вектора (3) помечены рёбрами сети.

### 1.2. Кодовое зашумление

Предположим, что имеется наблюдатель, который может подслушивать значения, передаваемые по $\mu \leqslant e(\mathcal{N})$ рёбрам сети $\mathcal{N}$. Пусть для защиты от такого наблюдения применяется метод кодового зашумления [7]. Опишем этот метод. Пусть $\mathcal{C}$ — линейный $(n, n-k)$-код с порождающей матрицей $G = G_{(n-k)\times n}$ и проверочной матрицей $H = H_{k\times n}$. Построим матрицу $\widetilde{G} = \widetilde{G}_{n\times n}$ вида

$$\widetilde{G} = \begin{pmatrix} G^* \\ G \end{pmatrix},$$

где $G^* = G^*_{k\times n}$ и $\mathrm{rank}(\widetilde{G}) = n$. Для кодирования информационного блока $\mathbf{s} \in \mathbb{F}_q^k$ случайным образом выбирается вектор $\mathbf{v} \in \mathbb{F}_q^{n-k}$ и выполняется операция

$$(\mathbf{s}||\mathbf{v})\widetilde{G} = \mathbf{s}G^* + \mathbf{v}G = \mathbf{x}. \tag{4}$$

Правило кодирования задаёт отображение

$$\mathbf{s} \mapsto C_{\mathbf{s}} = \mathbf{s}G^* + \mathcal{C},$$

которое каждому информационному блоку $\mathbf{s} \in \mathbb{F}_q^k$ ставит в соответствие фактор-класс $C_{\mathbf{s}}$ из фактор-множества $\mathbb{F}_q^n/\mathcal{C}$. Заметим, что за счёт случайного аргумента $\mathbf{v}$ в (4) один и тот же информационный блок $\mathbf{s}$ в разные моменты времени может быть закодирован, в общем случае, в разные кодовые векторы. Напомним, что кодовый вектор $\mathbf{x}$, полученный по правилу (4), по мнимым рёбрам загружается в источник $S$ сети $\mathcal{N}$.

Так как, по предположению, в сети $\mathcal{N}$ нет помех, каждый из $t$ легитимных получателей примет исходный вектор $\mathbf{x}$. Согласно [10], матрицу $H$ всегда можно выбрать так, что для любого информационного блока $\mathbf{s} \in \mathbb{F}_q^k$ и любого $\mathbf{x} \in C_{\mathbf{s}}$ справедливо равенство

$$\mathbf{x}H^{\mathrm{T}} = \mathbf{s}.$$

В соответствии с [10] код $\mathcal{C}$ будем называть базовым кодом, а код, построенный по $\mathcal{C}$, — факторным кодом и обозначать $(\mathbb{F}_q^n/\mathcal{C})$.

### 1.3. Модель $l$-кратного наблюдения

Пусть $\mathcal{C}$ — базовый $(n, n-k)$-код, $(\mathbb{F}_q^n/\mathcal{C})$ — соответствующий факторный код, $\mathbf{s} \in \mathbb{F}_q^k$ — информационный блок, $\mathbf{x}(1), \ldots, \mathbf{x}(l)$ — кодовые слова факторного кода $(\mathbb{F}_q^n/\mathcal{C})$, соответствующие информационному блоку $\mathbf{s}$ в моменты времени $1, \ldots, l$, $l \geqslant 1$. Случайный вектор, моделирующий множество информационных векторов, обозначим $\mathbf{S}$, а через $\mathbf{X}_i$ — случайный вектор, моделирующий кодовые векторы в момент времени $i$, $i \in \{1, \ldots, l\}$. Пусть $\mathcal{T}_i$ — множество рёбер, наблюдаемое в момент времени $i$, $i \in \{1, \ldots, l\}$, $\mathcal{T}_i \subseteq \mathcal{E}$, $|\mathcal{T}_i| = \mu_i$. Отметим, что множество $\{\mathcal{T}_i : i = 1, \ldots, l\}$ может содержать любые рёбра сети, в том числе и рёбра, по которым компоненты кодовых слов передаются в чистом виде, например мнимые рёбра. Тогда наблюдателю доступны для исследования частичные векторы значений $\mathcal{F}_{\mathcal{T}_1}(\mathbf{x}(1)), \ldots, \mathcal{F}_{\mathcal{T}_l}(\mathbf{x}(l))$, где в векторе $\mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i))$ длины $\mu_i$ координаты помечены рёбрами из $\mathcal{T}_i$ и для каждого $e \in \mathcal{T}_i$ координата с соответствующей меткой имеет значение $\widetilde{f}_e(\mathbf{x}(i))$, $i \in \{1, \ldots, l\}$ (см. (3)). Пусть для $i \in \{1, \ldots, l\}$ случайный вектор $\mathbf{Y}_{\mathcal{T}_i}(i)$ моделирует распределение соответствующего вектора значений вида $\mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i))$. Неопределённость наблюдателя при $l$-кратном подслушивании, соответствующем набору $\mathcal{T}_1, \ldots, \mathcal{T}_l$, определим естественным образом как условную энтропию

$$\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)). \tag{5}$$

В общем случае предполагается, что в сети существует наблюдатель, который может произвольно выбирать набор $\mathcal{T}_1, \ldots, \mathcal{T}_l$, $|\mathcal{T}_i| = \mu_i$, $i = 1, \ldots, l$. Поэтому введём обозначение для минимально возможной неопределённости наблюдателя при заданном наборе $(\mu_1, \ldots, \mu_l)$:

$$\Delta(\mu_1, \ldots, \mu_l) = \min_{\mathcal{T}_i \subset \mathcal{E}, |\mathcal{T}_i| = \mu_i, i \in \{1,\ldots,l\}} \{\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}\}. \tag{6}$$

В случае, когда $\mu_1 = \ldots = \mu_l = \mu$, величину $\Delta(\mu_1, \ldots, \mu_l)$ будем обозначать $\Delta^{(l)}(\mu)$.

## 2. Оценка меры неопределённости при $l$-кратном наблюдении

Предполагается, что наблюдателю известен факторный код, проверочная матрица базового кода и матрицы сетевых линейных преобразований вида (1) и (2). В случае, когда для всех $\mu_i$, $i \in \{1, \ldots, l\}$, выполняется равенство $\Delta(\mu_i) = k$, будем говорить, что обеспечена совершенная защита. Если же это равенство не выполняется для некоторых $j \in \{1, \ldots, l\}$, то наблюдатель может попытаться выбрать подмножества наблюдаемых рёбер так, чтобы максимально уменьшить множество претендентов. Отметим, что существенным отличием от перехвата в канале является то, что наблюдатель наблюдает не координаты векторов в чистом виде, а их линейные комбинации.

2.1. Случай $l = 1$

Пусть информационный вектор $\mathbf{s} \in \mathbb{F}_q^k$ кодируется с помощью факторного кода $(\mathbb{F}_q^n/\mathcal{C})$ в вектор $\mathbf{x} = (x_1, \ldots, x_n)$. При передаче по сети вектора $\mathbf{x}$ по рёбрам графа передаются компоненты $x_j$, $j \in \{1, \ldots, n\}$, и их линейные комбинации. Пусть $\mathcal{T}$ — множество наблюдаемых рёбер, $|\mathcal{T}| = \mu$, $H_1$ — матрица вида

$$H_1 = \left[\widetilde{\mathbf{f}}_{e_1}, \ldots, \widetilde{\mathbf{f}}_{e_\mu}\right],$$

где $e_i \in \mathcal{T}$, $i = 1, \ldots, \mu$. Другими словами, $H_1$ — матрица, состоящая из столбцов линейных преобразований вида (2) над координатами вектора $\mathbf{x}$, $r = \mathrm{rank}(H_1)$. Тогда после подслушивания наблюдателю доступен вектор $\mathbf{y}$ вида

$$\mathbf{y} = \mathcal{F}_{\mathcal{T}}(\mathbf{x}) = \mathbf{x}H_1.$$

Отметим, что наблюдателю известна матрица $H_1$ линейного преобразования координат и результат преобразования $\mathbf{y}$, а вектор $\mathbf{x}$ неизвестен. Без потери общности можно полагать, что ранг матрицы $H_1$ равен $\mu$, т. е. $r = \mu$. В противном случае подслушивание наблюдателя будет неоптимальным, так как какое-то из перехватываемых рёбер будет иметь значение, выражаемое линейно через другие перехватываемые значения. Поэтому как минимум одно из перехватываемых рёбер будет лишним. Таким образом, наблюдателю доступен для исследования вектор $\mathbf{y} \in \mathbb{F}_q^\mu$, составленный из наблюдаемых значений, передаваемых по $\mu$ рёбрам. Пусть $\mathcal{K}$ — $(n, n-r)$-код с проверочной матрицей $H_1^{\mathrm{T}}$. Для полноты изложения приведём простую лемму.

**Лемма 1.** Пусть $\mathcal{K}$, $\mathcal{C}$ — подпространства $\mathbb{F}_q^n$, $\widehat{\mathcal{C}} = \mathcal{K} \cap \mathcal{C}$. Если смежные классы $\mathfrak{a}$ из $\mathbb{F}_q^n/\mathcal{C}$ и $\mathfrak{b}$ из $\mathbb{F}_q^n/\mathcal{K}$ пересекаются, то $|\mathfrak{a} \cap \mathfrak{b}| = q^{\dim(\widehat{\mathcal{C}})}$.

***Доказательство.*** Так как $\widehat{\mathcal{C}} \subset \mathcal{C}$ и $\widehat{\mathcal{C}} \subset \mathcal{K}$, то можно построить разбиения подпространств $\mathcal{C}$ и $\mathcal{K}$: $\mathcal{C}/\widehat{\mathcal{C}}$, $\mathcal{K}/\widehat{\mathcal{C}}$. Смежные классы $\mathfrak{a} \in \mathcal{C}/\widehat{\mathcal{C}}$ и $\mathfrak{b} \in \mathcal{K}/\widehat{\mathcal{C}}$ представим в следующем виде:

$$\mathfrak{a} = \bigcup_{\widetilde{a}} \{\widetilde{a} + \widehat{\mathcal{C}}\}, \quad \mathfrak{b} = \bigcup_{\widetilde{b}} \{\widetilde{b} + \widehat{\mathcal{C}}\},$$

где $\widetilde{a} \in \mathcal{C} \setminus \widehat{\mathcal{C}}$; $\widetilde{b} \in \mathcal{K} \setminus \widehat{\mathcal{C}}$. Так как смежный класс $\mathfrak{a}$ из $\mathbb{F}_q^n/\mathcal{C}$ пересекается со смежным классом $\mathfrak{b}$ из $\mathbb{F}_q^n/\mathcal{K}$, то существуют $\widetilde{a} \in \mathcal{C} \setminus \widehat{\mathcal{C}}$, $\widetilde{b} \in \mathcal{K} \setminus \widehat{\mathcal{C}}$, $\widehat{c}_1, \widehat{c}_2 \in \widehat{\mathcal{C}}$, такие, что $\widetilde{a} + \widehat{c}_1 = \widetilde{b} + \widehat{c}_2$. Тогда для всех $\widehat{c} \in \widehat{\mathcal{C}}$ справедливо равенство $\widetilde{a} + \widehat{c}_1 + \widehat{c} = \widetilde{b} + \widehat{c}_2 + \widehat{c}$. Следовательно, $|\mathfrak{a} \cap \mathfrak{b}| = q^{\dim(\widehat{\mathcal{C}})}$. ■

**Следствие 1.** Пусть $\mathcal{K}$, $\mathcal{C}$ — подпространства $\mathbb{F}_q^n$, $\widehat{\mathcal{C}} = \mathcal{K} \cap \mathcal{C}$. Тогда каждый смежный класс из $\mathbb{F}_q^n/\mathcal{K}$ пересекается с $q^{\dim(\mathcal{K}) - \dim(\widehat{\mathcal{C}})}$ смежными классами из $\mathbb{F}_q^n/\mathcal{C}$.

**Теорема 1.** Пусть $\mathcal{T}$ — множество наблюдаемых рёбер, $|\mathcal{T}| = \mu$, $H_1$ — соответствующая множеству $\mathcal{T}$ матрица линейных преобразований вида (2.1), $\mathcal{K}$ — линейный код с проверочной матрицей $H_1$, $\mathcal{C}$ — базовый код факторного кода $(\mathbb{F}^n/\mathcal{C})$. Тогда

$$\Delta_{\mathcal{T}} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}}) = \dim(\mathcal{K}) - \dim(\mathcal{K} \cap \mathcal{C}). \tag{7}$$

***Доказательство.*** Воспользуемся определением энтропии:

$$\mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}}) = \sum_{\mathbf{y} \in \mathbb{F}^\mu} p(\mathbf{y}) H(\mathbf{S}|\mathbf{y}) = -\sum_{\mathbf{y} \in \mathbb{F}^\mu} \sum_{\mathbf{s} \in \mathbb{F}^k} p(\mathbf{y}) p(\mathbf{s}|\mathbf{y}) \log p(\mathbf{s}|\mathbf{y}),$$

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = \sum_{\mathbf{s} \in \mathbb{F}^k} p(\mathbf{s}|\mathbf{y}) I(\mathbf{s}|\mathbf{y}) = -\sum_{\mathbf{s} \in \mathbb{F}^k} p(\mathbf{s}|\mathbf{y}) \log p(\mathbf{s}|\mathbf{y}).$$

Пусть $\mathbf{y}$ — конкретный вектор наблюдаемых значений, а $\mathbf{s}$ — конкретный информационный вектор. Представим $p(\mathbf{s}|\mathbf{y})$ в виде

$$p(\mathbf{s}|\mathbf{y}) = \frac{p(\mathbf{s},\mathbf{y})}{p(\mathbf{y})} = \frac{p(\mathbf{y}|\mathbf{s})p(\mathbf{s})}{p(\mathbf{y})}.$$

Так как все информационные блоки появляются с одинаковой вероятностью, $p(\mathbf{s}) = 1/q^k$. Найдём $p(\mathbf{y}|\mathbf{s})$:

$$p(\mathbf{y}|\mathbf{s}) = \sum_{\mathbf{x}\in C_{\mathbf{s}}} p(\mathbf{x}|\mathbf{s})p(\mathbf{y}|\mathbf{x}) = \frac{1}{q^{(n-k)}} \sum_{\mathbf{x}\in C_{\mathbf{s}}\cap K_{\mathbf{y}}} p(\mathbf{y}|\mathbf{x}) = \frac{|C_{\mathbf{s}}\cap K_{\mathbf{y}}|}{q^{(n-k)}},$$

где $K_{\mathbf{y}}$ — смежный класс из $\mathbb{F}^n/\mathcal{K}$, соответствующий синдрому $\mathbf{y}$. Так как $\operatorname{rank}(H_1) = r$ и $\mathbf{y} = \mathbf{x}H_1$, легко проверить, что $p(\mathbf{y}) = 1/q^r$. В итоге получим

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = -\sum_{\mathbf{s}\in S} p(\mathbf{s}|\mathbf{y})\log p(\mathbf{s}|\mathbf{y}) = -\sum_{s\in S} q^{r-n}|C_{\mathbf{s}}\cap K_{\mathbf{y}}|\log_q(q^{r-n}|C_{\mathbf{s}}\cap K_{\mathbf{y}}|).$$

По лемме 1 $|C(\mathbf{s})\cap K(\mathbf{y})| = |\mathcal{C}\cap\mathcal{K}| = q^{\dim(\mathcal{C}\cap\mathcal{K})}$, поэтому

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = -\sum_{\mathbf{s}\in\mathbb{F}^k} q^{r-n}q^{\dim(\mathcal{C}\cap\mathcal{K})}((r-n)+\dim(\mathcal{C}\cap\mathcal{K})) = \\ = -\sum_{\mathbf{s}\in\mathbb{F}^k} q^{r-n+\dim(\mathcal{C}\cap\mathcal{K})}(r-n+\dim(\mathcal{C}\cap\mathcal{K})).$$

По следствию 1 имеем, что для заданного вектора наблюдаемых значений $\mathbf{y}$ имеется $q^{n-r-\dim(\mathcal{C}\cap\mathcal{K})}$ кандидатов на информационный блок. Поэтому

$$\mathrm{H}(\mathbf{S}|\mathbf{y}) = -q^{r-n+\dim(\mathcal{C}\cap\mathcal{K})}q^{n-r-\dim(\mathcal{C}\cap\mathcal{K})}(r-n+\dim(\mathcal{C}\cap\mathcal{K})) = \\ = n-r-\dim(\mathcal{C}\cap\mathcal{K}) = \dim(\mathcal{K}) - \dim(\mathcal{K}\cap\mathcal{C}).$$

Так как $\mathrm{H}(\mathbf{S}|\mathbf{y})$ не зависит от $\mathbf{y}$, то $\mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}}) = \dim(\mathcal{K}) - \dim(\mathcal{K}\cap\mathcal{C})$. ■

Полученный в теореме 1 результат можно обобщить на случай, когда множество $\mathcal{T}$ неизвестно, а известно только то, что наблюдатель может выбирать произвольное множество мощности $\mu$. В этом случае, с точки зрения защиты, необходимо знать гарантированный уровень неопределённости при заданном $\mu$. Пусть $\mathcal{H}(\mu)$ — множество всех $(n\times\mu)$-матриц линейных преобразований, которые можно построить по $\mu$ ребрам сети; $\mathcal{K}(\mu)$ — множество всех линейных кодов, для каждого из которых найдется проверочная матрица из $\mathcal{H}(\mu)$. Тогда из (6) получим

$$\Delta(\mu) = \min_{K\in\mathcal{K}(\mu)}\{\dim(K) - \dim(K\cap\mathcal{C})\}.$$

### 2.2. Случай $l > 1$

Далее для удобства набор кодовых векторов $\mathbf{x}(1),\ldots,\mathbf{x}(l)\in\mathbb{F}_q^n$, соответствующий одному информационному блоку $\mathbf{s}\in\mathbb{F}_q^k$, назовём однородной выборкой объёма $l$.

**Теорема 2.** Пусть наблюдателю доступна однородная выборка объёма $l$, $\mathcal{T}_i$ — подмножество подслушиваемых рёбер в момент времени $i$, $|\mathcal{T}_i| = \mu_i$, $H_i$ — соответствующая множеству $\mathcal{T}_i$ матрица линейных преобразований:

$$H_i = \left[\widetilde{\mathbf{f}}_{e_{i,1}},\ldots,\widetilde{\mathbf{f}}_{e_{i,\mu_i}}\right].$$

Здесь $e_{i,j} \in \mathcal{T}_i$, $j \in \{1,\ldots,\mu_i\}$; $\widetilde{\mathbf{f}}_{e_{i,j}}$ — глобальное кодирующее отображение для ребра $e_{i,j} \in \mathcal{T}_i$, $i \in \{1,\ldots,l\}$; $\mathcal{C}$ — базовый код факторного кода $\mathbb{F}^n/\mathcal{C}$. Тогда

$$\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = k + \dim(\mathcal{L}(M_1) \cap \mathcal{L}(M_2)) - \sum_{i=1}^{l} \dim(\mathcal{C}^\perp \cap \mathcal{L}(H_i^{\mathrm{T}})), \tag{8}$$

где

$$M_1 = \begin{pmatrix} H_1^{\mathrm{T}} & 0 & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & H_l^{\mathrm{T}} \end{pmatrix}; \quad M_2 = \begin{pmatrix} H & -H & 0 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ H & 0 & 0 & \ldots & 0 & -H \end{pmatrix};$$

$\mathcal{L}(A)$ — линейная оболочка, натянутая на строки матрицы $A$.

***Доказательство.*** После $l$-го подслушивания наблюдателю доступны векторы $\mathbf{y}(i)$ следующего вида:

$$\mathbf{y}(i) = \mathcal{F}_{\mathcal{T}_i}(\mathbf{x}(i)) = \mathbf{x}(i)H_i, \quad i = 1,\ldots,l. \tag{9}$$

Из формулы (5) получим

$$\begin{gathered} \Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) = \mathrm{H}(\mathbf{S}|\mathbf{X}_1,\ldots,\mathbf{X}_l,\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) + \\ + \mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) - \mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{S},\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) = \\ = \mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) - \mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{S},\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)). \end{gathered}$$

Вычислим каждое из слагаемых в последнем равенстве. Пусть $(\mathbf{x}(1),\ldots,\mathbf{x}(l))$ — какая-то реализация для набора случайных векторов $\mathbf{X}_1,\ldots,\mathbf{X}_l$. По условию теоремы векторы $\mathbf{x}(1)$, ..., $\mathbf{x}(l)$ соответствуют одному информационному блоку, т. е. принадлежат одному смежному классу. Поэтому выполняются следующие равенства:

$$H\left[\mathbf{x}^{\mathrm{T}}(1) - \mathbf{x}^{\mathrm{T}}(i)\right] = 0, \quad i \in \{2,\ldots,l\}. \tag{10}$$

Перепишем равенства (9) и (10) вместе в матричном виде:

$$M\left[\mathbf{x}(1),\ldots,\mathbf{x}(l)\right]^{\mathrm{T}} = [\mathbf{y}(1),\ldots,\mathbf{y}(l),\underbrace{0,\ldots,0}_{l-1}]^{\mathrm{T}}, \tag{11}$$

где $M = \begin{pmatrix} M_1 \\ M_2 \end{pmatrix}$. Мощность множества решений системы (11) равна $q^{ln-\mathrm{rank}(M)}$. Таким образом, $\mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) = ln - \mathrm{rank}(M)$, где

$$\mathrm{rank}(M) = \sum_{i=1}^{l} \mathrm{rank}(H_i^{\mathrm{T}}) + (l-1)\,\mathrm{rank}(H) - \dim(\mathcal{L}(M_1) \cap \mathcal{L}(M_2)).$$

Вычислим $\mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{S},\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l))$. Так как при фиксированном $\mathbf{s}$ случайные векторы $\mathbf{X}_i$ и $\mathbf{Y}_j$, $i \neq j$, независимы, получим

$$\mathrm{H}(\mathbf{X}_1,\ldots,\mathbf{X}_l|\mathbf{S},\mathbf{Y}_{\mathcal{T}_1}(1),\ldots,\mathbf{Y}_{\mathcal{T}_l}(l)) = \sum_{i=1}^{l} \mathrm{H}(\mathbf{X}_i|\mathbf{S},\mathbf{Y}_{\mathcal{T}_i}(i)). \tag{12}$$

Отметим, что для $i \in \{1,\ldots,l\}$

$$\begin{gathered} \mathrm{H}(\mathbf{X}_i|\mathbf{S},\mathbf{Y}_{\mathcal{T}_i}(i)) = \mathrm{H}(\mathbf{X}_i|\mathbf{Y}_{\mathcal{T}_i}(i)) - \mathrm{H}(\mathbf{S}|\mathbf{Y}_{\mathcal{T}_i}(i)) = \\ = \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}})) - (\dim(\mathcal{L}^\perp(H_i^{\mathrm{T}})) - \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}}) \cap \mathcal{C})) = \dim(\mathcal{L}^\perp(H_i^{\mathrm{T}}) \cap \mathcal{C}) = n - \mathrm{rank}\begin{pmatrix} H \\ H_i^{\mathrm{T}} \end{pmatrix}. \end{gathered}$$

Следовательно, принимая во внимание (12), получаем

$$\mathrm{H}(\mathbf{X}_1, \ldots, \mathbf{X}_l | \mathbf{S}, \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = \sum_{i=1}^{l} \left( n - \operatorname{rank} \begin{pmatrix} H \\ H_i^{\mathrm{T}} \end{pmatrix} \right) =$$
$$= ln - l \cdot \operatorname{rank}(H) - \sum_{i=1}^{l} \left[ \operatorname{rank}(H_i^{\mathrm{T}}) - \dim(\mathcal{C}^{\perp} \cap \mathcal{L}_{H_i^{\mathrm{T}}}) \right].$$

Собирая полученные выражения, запишем

$$\mathrm{H}(\mathbf{S} | \mathbf{Y}_{\mathcal{T}_1}(1), \ldots, \mathbf{Y}_{\mathcal{T}_l}(l)) = \operatorname{rank}(H) + \dim(\mathcal{L}(M_1) \cap \mathcal{L}(M_2)) - \sum_{i=1}^{l} \dim(\mathcal{C}^{\perp} \cap \mathcal{L}(H_i^{\mathrm{T}})).$$

Теорема доказана. ■

Отметим, что порядок подслушивания множеств $\mathcal{T}_i$ не влияет на значение неопределённости $\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}$. Ценным с практической точки зрения следствием представляется тот факт, что если матрицы сетевых линейных преобразований совпадают, то никакое повторное наблюдение не принесёт дополнительной информации.

**Следствие 2.** Если $\mathcal{L}(H_i^{\mathrm{T}}) = \mathcal{L}(H_1^{\mathrm{T}})$ для всех $i \in \{1, \ldots, l\}$, то $\Delta_{\mathcal{T}_1} = \Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}$.

***Доказательство.*** Вычислим $\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}$:

$$\Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l} = k + (l-1)\dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H)) - l \dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H)) =$$
$$= k - \dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H)).$$

С другой стороны, согласно (7),

$$\Delta_{\mathcal{T}_1} = \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) - \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}}) \cap \mathcal{L}^{\perp}(H)) =$$
$$= \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) - [\dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}})) + \dim(\mathcal{L}^{\perp}(H)) - \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}}) \cup \mathcal{L}^{\perp}(H)) =$$
$$= \dim(\mathcal{L}^{\perp}(H_1^{\mathrm{T}}) \cup \mathcal{L}^{\perp}(H)) - \dim(\mathcal{L}^{\perp}(H)) =$$
$$= n - \dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H)) - [n-k] = k - \dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H)) = \Delta_{\mathcal{T}_1,\ldots,\mathcal{T}_l}.$$

Следствие доказано. ■

Следствие 2, в частности, может позволить подстраивать защиту информации в сети в тех ситуациях, когда наблюдатель не может по своему усмотрению выбирать множества подслушиваемых рёбер.

Из следствия 2 получаем, что если наблюдатель подслушивает рёбра из множества $\mathcal{T}$ мощности $\mu$, то $\Delta_{\mathcal{T}} = k - \dim(\mathcal{L}(H_1^{\mathrm{T}}) \cap \mathcal{L}(H))$. Если, как и раньше, $\operatorname{rank}(H_1) = \mu$, то минимальное значение величины $\Delta_{\mathcal{T}}$ равно $\Delta^{\mu,\min} = k - \min\{k, \mu\}$, а максимальное — $\Delta^{\mu,\max} = k - \max\{0, \mu - (n-k)\}$. Используя $\Delta^{\mu,\min}$ и $\Delta^{\mu,\max}$, можно получить грубую оценку $\bar{l}(\mu)$ количества перехватов в сети, после которых мера неопределённости $\Delta^{(l)}(\mu)$ будет равна нулю. Для этого воспользуемся формулой (1.23) из [11, с. 38] и получим

$$\left\lceil \left(1 - \log_{|\mathbb{F}_q^k|-1}\left(q^{\Delta^{\mu,\min}} - 1\right)\right)^{-1} \right\rceil \leqslant \bar{l}(\mu) - 1 \leqslant \left\lceil \left(1 - \log_{|\mathbb{F}_q^k|-1}\left(q^{\Delta^{\mu,\max}} - 1\right)\right)^{-1} \right\rceil. \quad (13)$$

## 2.3. Пример вычисления меры неопределённости

Рассмотрим сеть, изображенную на рис. 1. Пусть $(\mathbb{F}_2^8/\mathcal{C})$ — факторный код, где $\mathcal{C}$ — самодуальный код Рида — Маллера с проверочной матрицей

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

Пусть в сети на вход источника $S$ по мнимым рёбрам загружается кодовое слово $\mathbf{x} = (x_1, \ldots, x_8)$ факторного кода $(\mathbb{F}_2^8/\mathcal{C})$; в узлах $C$, $F$, $I$ и $L$ выполняется суммирование (в поле $\mathbb{F}_2$) приходящих по входным рёбрам битов.

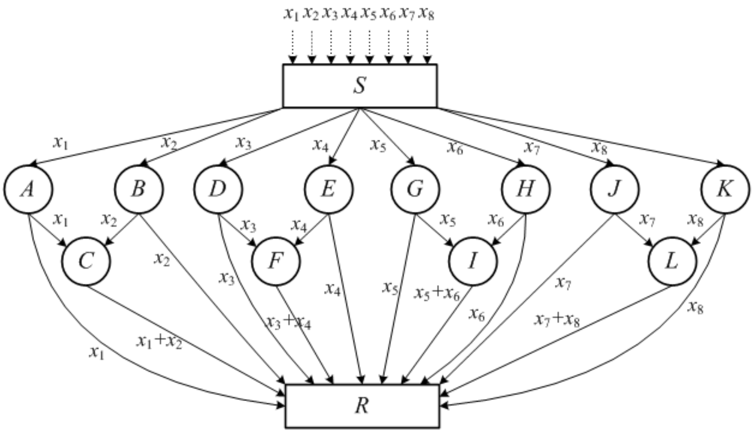


Рис. 1. Сеть с кодированием в узлах $C$, $F$, $I$, $L$

Для данной сети вычислена неопределенность $\Delta^{(l)}(\mu)$ наблюдателя для $l$-кратного подслушивания в зависимости от $\mu$. Результаты вычислений, приведённые в таблице, показывают, что при $\mu = 1$ повторный перехват при любом $l$ не позволяет снизить неопределённость меньше 4. То есть в этом случае обеспечивается совершенная защита даже при $l$-кратном подслушивании при любом $l$. В то же время при $\mu = 2$ необходимо и достаточно четырёх повторных перехватов для полного снятия неопределённости. Примером такой последовательности перехватываемых рёбер может быть последовательность $(\{CR, FR\}, \{CR, IR\}, \{CR, LR\}, \{IR, LR\})$.

**Результаты вычисления** $\Delta^{(l)}(\mu)$

| | | $\mu$ | | | |
|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** |
| $l$ | **1** | 4 | 3 | 1 | 0 |
| | **2** | 4 | 2 | 0 | 0 |
| | **3** | 4 | 1 | 0 | 0 |
| | **4** | 4 | 0 | 0 | 0 |

Воспользуемся оценкой (13) для этого примера. Непосредственные вычисления показывают, что при $\mu = 1$ значение величины $\bar{l}(\mu)$ лежит в границах от $\infty$ до $\infty$ (значение дроби $1/0$ здесь и далеее полагается равным $\infty$), что соответствует точному результату, согласно которому совершенная защита при $l$-кратном подслушивании обеспечивается при всех $l$. В то же время при $\mu = 2$ получим $3 \leqslant \bar{l}(\mu) \leqslant \infty$; из таблицы видно, что полностью неопределённость снимается при $l = 4$. При $\mu = 3$ нижняя оценка $\bar{l}(\mu) = 2$ совпадает с точным значением $l$, при котором неопредёленность снимается полностью.

Отметим, что, помимо грубой оценки (13) для $\Delta^{(l)}(\mu)$, представляет интерес аналитическое уточнение формулы вычисления меры неопредёленности $\Delta(\mu_1, \ldots, \mu_l)$ для конкретных базовых и сетевых кодов, так как по полученной в работе формуле (8) эта мера может быть вычислена только алгоритмически перебором всех возможных наборов подмножеств подслушиваемых рёбер. В [12] получена формула вычисления меры стойкости кодового зашумления в случае, когда данные многократно передаются по каналу, а не по линейной сети. Там же эту формулу удалось аналитически уточнить только в частных случаях для базового кода Хэмминга и некоторых кодов Рида — Маллера. Уточнение формулы (8) представляется задачей не менее трудной, чем уточнение аналогичной формулы, полученной в [12], так как канал можно рассматривать как тривиальный случай линейной сети.

## ЛИТЕРАТУРА

1. *Габидулин Э. М., Пилипчук Н. И., Колыбельников А. И. и др.*Сетевое кодирование // Труды МФТИ. 2009. Т. 1. № 2. С. 3–25.
2. *Yeung R. W. and Zhang Z.* Distributed source coding for satellite communications // IEEE Trans. Inform. Theory. 1999. V. 1. No. 45. P. 1111–1120.
3. *Ahlswede R., Cai N., Li S. R., and Yeung R. W.* Network information flow // IEEE Trans. Inform. Theory. 2000. V. 46. No. 6. P. 1204–1216.
4. *Бараш Л. С.* Сетевое кодирование // Компьютерное обозрение. 2009. Т. 5. № 671. С. 20–31.
5. *Rouayheb S. E. and Soljanin E.* On wiretap networks II // Proc. 2007 IEEE Intern. Symp. (ISIT-2007). Nice, France, 24–29 June 2007. P. 551–555.
6. *Rouayheb S. E., Soljanin E., and Sprinston A.* Secure network coding for wiretap networks of type II // IEEE Trans. Inform. Theory. 2012. V. 58. No. 3. P. 1361–1371.
7. *Ozarov H. and Wyner A. D.* Wire-Tap Channel II // BLTj. 1984. V. 63. No. 10. P. 2135–2157.
8. *Винничук И. И., Газарян Ю. О., Косолапов Ю. В.* Стойкость кодового зашумления в рамках модели многократного частичного наблюдения кодовых сообщений // Материалы XII Междунар. науч.-практич. конф. «Информационная безопасность». Таганрог: Известия ЮФУ, 2012. С. 258–263.
9. *Yeung R. W., Li S. R., Cai N., et al.* Network coding theory, foundation and trends // Communic. Inform. Theory. 2005. V. 2. No. 4. C. 241–381.
10. *Деундяк В. М., Косолапов Ю. В.* Математическая модель канала с перехватом второго типа // Изв. вузов. Северо-Кавказский регион, сер. Естественные науки. 2008. Т. 3. № 145. С. 3–8.
11. *Шанкин Г. П.* Ценность информации. Вопросы теории и приложений. М.: Филоматис, 2004. 128 с.
12. *Деундяк В. М., Косолапов Ю. В.* Об одном методе снятия неопределенности в канале с помехами в случае применения кодового зашумления // Известия ЮФУ. Технические науки. 2014. Т. 2. № 151. С. 197–208.