УДК 621.391

СЕТЕВОЕ КОДИРОВАНИЕ КОДОМ РИДА-СОЛОМОНА С УЧЕТОМ ЛИДЕРОВ СТОХАСТИЧЕСКОЙ СЕТИ

С.Б. САЛОМАТИН, А.Э. АЛЕКСЕЕНКО, А.П. ТУРЛАЙ

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 8 марта 2021

Аннотация. Рассмотрены алгоритмы сетевого кодирования в линейной стохастической сети с использованием лидеров сети. Приведены модели поиска лидеров, алгоритмы кодирования и декодирования кода Рида-Соломона с исправлением ошибок и стираний. Приведены результаты моделирования.

Ключевые слова: лидеры стохастической линейной сети, алгоритмы поиска, код Рида-Соломона, декодирование ошибок и стираний

Введение

Известные методы и алгоритмы сетевого кодирования [1–2] позволяют улучшить надежность работы стохастических сенсорных сетей. В гомогенных сетях с разными состояниями узлом сети этого может оказаться недостаточно.

Одним из путей повышения эффективности работы стохастических сенсорных сетей является применение алгоритма кодирования пакетов сети с указанием лидера сети, имеющего наилучшее управление пространством состояний, и кодов, корректирующих ошибки и стирания.

1. Модель динамической стохастической сенсорной сети

Мы рассматриваем сети, в которых каждый узел обновляет скалярное состояние $\dot{\psi}_i$, $\dot{\psi} = u_i + w_i$, $i = 1,...,n$, где u_i – управляющий вход и w_i – белое стохастическое возмущение с нулевым средним и единичной дисперсией. Узел является последовательным, если для формирования управляющего действия используется только относительный обмен информацией с соседями $u_i = -\sum_{j \in N_i} \left(\psi_i - \psi_j \right)$.

Узел является *лидером*, если, помимо относительного обмена информацией с соседями, он также имеет доступ к собственному состоянию

$$u_i = -\sum_{j \in N_i} \left(\psi_i - \psi_j \right) - k_i \psi_i,$$

где k_i – положительное число и N_i является набором всех узлов, с которыми связывается узел i. Таким образом, представление пространства-состояния лидера согласованной сети задается уравнением

$$\dot{\psi} = -\left(L + \mathrm{diag}\left(\mathbf{k}\right) \mathrm{diag}\left(\mathbf{x}\right) \right) \psi + w,$$

где $\mathbf{x}$ – вектор с логическим значением с i-ого элемента $x_i \in \{0,1\}$, указывающей, что узел i является лидером, если $x_i = 1$ и что узел i является последовательным, если $x_i = 0$.

Ковариационная матрица в установившемся режиме имеет вид $\sigma = \lim_{t \to \infty} M\left(\psi(t) \psi^T(t) \right)$ и может быть определена с помощью уравнения Ляпунова:

$$\left(L+\mathrm{diag}\left(k\right)\mathrm{diag}\left(x\right)\right)\sigma+\sigma\left(L+\mathrm{diag}\left(k\right)\mathrm{diag}\left(x\right)\right)=I.$$

где $M\left(\cdot\right)$, $M\left(w(t)w^T\left(\tau\right)\right)=I\delta\left(y=\tau\right)$ – оператор математического ожидания, $\sigma=\frac{1}{2}\left(L+\mathrm{diag}\left(k\right)\mathrm{diag}\left(x\right)\right)^{-1}$.

Дисперсия стационарного режима в общем виде определяется как $\mathrm{trace}\left(\sigma\right)=\frac{1}{2}\mathrm{trace}\left(\left(L+\mathrm{diag}\left(\mathbf{k}\right)\mathrm{diag}\left(\mathbf{x}\right)\right)^{-1}\right)$ и количественно определяет величину отклонение от согласованного режима стохастических сетей. Таким образом, проблема идентификации лидеров сети, сводится к решению задачи минимизации среднеквадратического отклонения по алгоритмам МНК следующего вида

$$\text{minimize} \quad J\left(x\right)=\mathrm{trace}\left(\left(L+\mathrm{diag}\left(k\right)\mathrm{diag}\left(x\right)\right)^{-1}\right),$$

$$\text{subject to} \quad x_i\in\left\{0,1\right\},\ \ i=1,...,n,$$

$$\sum_{i=1}^{n}x_i=N_l,$$

где граф Лапласиана L и вектор k с положительными элементами являются исходными данными задачи, а логически значимый вектор x с кардинальностью является переменной оптимизации.

Для сенсорных сетей МНК является эквивалентным задаче выбора абсолютных измерений положения среди n датчиков с минимальной дисперсией ошибки оценки [2].

Пример работы алгоритма показан на рис. 1.

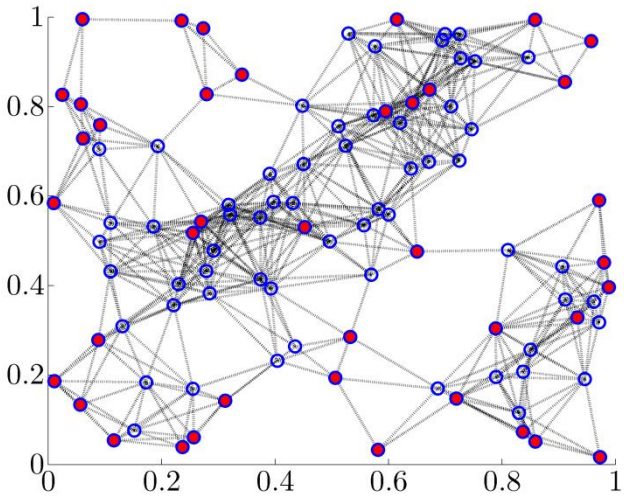

Рис. 1. Выбор лидеров стохастической сети, $J=0,95$

2. Модель сетевого кодирования

Модель сети состоит из источника, нескольких приемников, и промежуточных узлов. Источник осуществляет кодирование, а приемники декодирование сетевого кода. Вычисления выполняются в конечном поле $GF\left(q^m\right)$.

Исходная информация представляется в виде информационных векторов длины k над полем Галуа $GF\left(q^m\right)$, где q – степень простого числа. Каждый вектор поступает от источника на вход кодера сетевого канала. В процессе кодирования формируется набор векторов длины n.

Модель сетевого канала предполагает, что сетевой канал может порождать ошибки в виде передачи базисного вектора и стирания – исчезновение базисного вектора. В сетевых узлах производятся неизвестные линейные комбинации над полем $GF(q)$.

Декодер преобразует (декодирует) принятый набор векторов и определяет информационный вектор длины *k*.

Кодер сопоставляет информационному вектору подпространство, и передает по сети композицию базисных векторов. Предполагается, что линейные комбинации в узлах не выводят векторы из подпространства. Линейные комбинации в узлах случайные, что может приводить к получению порождающей системы вложенного в исходное подпространства (рис. 2).

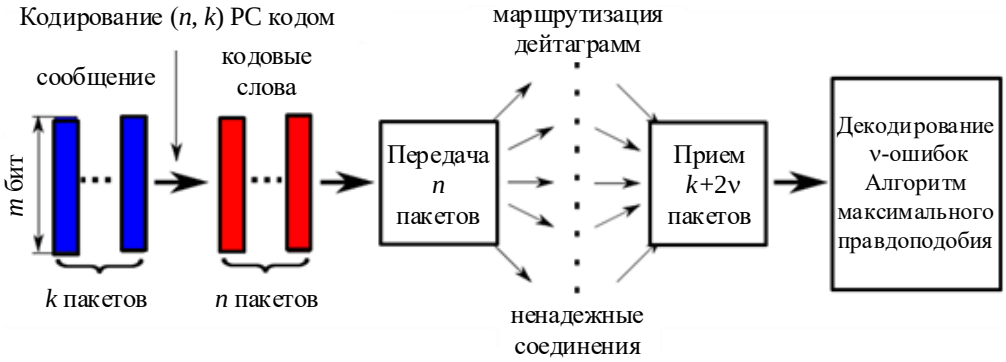

Рис. 2. Схема сетевого кодирования с использованием кода Рида-Соломона

Рассмотрим конечное поле $GF(q)$ и его расширение $GF\left(q^m\right)$, которое иногда будет удобно представлять как векторное пространство $GF\left(q^m\right)^n$. Выберем некоторое множество $A=\{\alpha_1,\alpha_2,...,\alpha_l\}$ линейно независимых над $GF(q)$ элементов $GF\left(q^m\right)^n$. Кодирование будет выглядеть следующим образом.

Пусть $\mathbf{a}=(a_0,a_1,...,a_{k-1})\in GF\left(q^m\right)^k$ – информационное сообщение.

Вектору **a** ставится в соответствие линеаризованный полином

$$a(x)=\sum_{l=0}^{k-1}a_i x^{q^i}\in GF\left(q^m\right)[x].$$

Для полинома $a(x)$ во всех точках $\{\alpha_i\}$ множества *A* вычисляется его значение β_i. Пары (α_i,β_i) можно рассматривать как элементы $GF(q)^{2m}$ пространства $W=A\oplus F_q^m$ размерности $(l+m)$. Множество пар $\{(\alpha_1,\beta_1),(\alpha_2,\beta_2),...,(\alpha_l,\beta_l)\}$ являются линейно независимыми над полем $GF(q)$ и образуют *l*-мерное пространство.

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 $GF(256)$ РС-код (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 заменяют символы с координатами стираний на нулевые символы. Для нового вектора находится полином синдрома стираний $s(x)$.

3. Определяется модифицированный полином синдрома

$$SE(x) = \left(\Gamma(x)\left[1 + s(x)\right] - 1\right) \bmod x^{2t+1}.$$

4. Вычисляется полином локаторов ошибок $\sigma(x)$, используя для этого алгоритм 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 $\omega(x) = \sigma(x)\left[1 + SE(x)\right] \bmod x^{2t+1}$ и определяется полином локаторов ошибок-стираний $\psi(x) = \sigma(x)\Gamma(x)$.

7. Оцениваются значения ошибок и стираний. Значения ошибок вычисляют по формуле

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

где ψ' – формальная производная.

Значения стираний вычисляют по формуле $F_{i_k} = \dfrac{-Y_k \omega\left(Y_k^{-1}\right)}{\psi'\left(Y_k^{-1}\right)}$.

3. Моделирование

Алгоритмы кодирования и поиска лидеров стохастической сети были промоделированы в среде Matlab. Результаты моделирования показали, что применение предлагаемых алгоритмов позволяет уменьшить вероятность ошибки при приеме пакетов сети. Такт для сети с параметрами $m = 4000$ – длина пакета, $k = 80$ пакетов на сообщение, $p = 0,03$ вероятности приема поврежденного пакета, вероятность ошибки $P_{err} = 10^{-4}$, тогда как для сети без кодирования $P_{err} = 0,9$.

Заключение

Применение сетевого кодирования с использованием лидеров стохастической сети и кода Рида-Соломона позволяет повысить надежность работы стохастической сети.

NETWORK CODING BY REED-SOLOMON CODE WITH STOCHASTIC NETWORK LEADING

S.B. SALOMATIN, A.E. ALEKSEENKO, A.P. TURLAY

Annotation. The algorithms of network coding in a linear stochastic network with the use of network leaders were considered. Lead search models, Reed-Solomon code coding and decoding algorithms with error correction and erasure were given. Simulation results were presented.

Keywords: stochastic line network leaders, search algorithms, Reed-Solomon code, error decoding and erasure

Список литературы

1. Martınez-Penas U., Kschischang F.R. Reliable and Secure Multishot Network Coding using Linearized Reed-Solomon Codes [Электронный ресурс]. URL: https://arXive:1805.03789v3[csIT].
2. Lin F., Fardad M., Jovanovi´c. R. // IEEE Transactions on automatic control. 2014. Vol. 59, № 7.