

ВЕРОЯТНОСТНО-АЛГЕБРАИЧЕСКОЕ КОДИРОВАНИЕ МАРШРУТА В СЕНСОРНОЙ СЕТИ

С.Б. САЛОМАТИН, А.А. ОХРИМЕНКО

Для реализации сетевого кодирования необходимо, чтобы каждый узел сети имел возможность вычислять линейные комбинации входящих пакетов и передавать их дальше. Это позволяет сделать работу сети более устойчивой.

Рассматривается алгебраический подход к кодированию пути пакета в сети. Основная идея кодирования состоит в том, что любой полином $f(x)$ степени d в поле $GF(p)$ может быть восстановлен по уникальным значениям вычисленных в $(d+1)$ точках.

Схема кодирования полного пути использует полином следующего вида $f_p(x) = (A_n x^{n-1} + A_{n-1} x^{n-2} + \dots + A_2 x + A_1) \bmod p$, где A_j — адрес промежуточного узла. Ассоциируем id-код j -го пакета со случайным числом x_j . Множество $\{x_j\}$ формируется генератором хаотических псевдослучайных чисел на основе сдвигов модулярных кодов разностного множества, что обеспечивает устойчивую идентификацию узлов сети.

Значение $f_p(x_j)$ является оценкой пройденного пути и в конечной точке полином f_p может быть реконструирован с помощью процедуры интерполяции.

Примем, что каждый j -й промежуточный узел вычисляет путь $P_{j,l}$ по формуле $P_{j,l} = P_{j-1,l} x_l + A_j$. Тогда решение уравнения, использующего матрицу Вандермонда, элементами которой являются различные значения $\{x_j\}$, вектор, состоящий из A_j , а также вектор $\{P_{j,l}\}$ дает оценку полного пути в точке назначения пакета.

Рандомизация алгоритма предполагает дополнительный учет вероятностного распределение по соседним узлам сети. Это распределение

основано на относительной вероятности того, что данный сосед передаст и, в конечном счете, доставит сообщение до адресата. Передача сообщений сама по себе обеспечивает отклик для корректировки вероятностного распределения. Подписанное подтверждение о доставке сообщения будет являться положительным откликом о достижимости пути. Система вероятностной маршрутизации при этом становится самокорректирующей.