

РАСПОЗНАВАНИЕ ТРАФИКА БЕСПРОВОДНОЙ КОМПЬЮТЕРНОЙ СЕТИ НА ФИЗИЧЕСКОМ УРОВНЕ

Национальный авиационный университет

Предложен метод анализа трафика беспроводной компьютерной сети на физическом уровне. Передаваемые данные предлагается представлять в виде функциональной зависимости с последующим разложением в ряд Фурье.

Актуальность темы

Постоянно возрастающее количество передаваемых данных через компьютерные сети вызывает необходимость проведения анализа трафика для целей обнаружения несанкционированных действий в сети, исследования работы сети для последующего усовершенствования, обнаружения неисправных участков сети для устранения неисправностей и т.д.

Необходимость системного подхода к проблеме распознавания данных обуславливается рядом причин. Первая состоит в том, что распознавание является средством получения информации, необходимой системе управления сетью (MNP) для выработки определенного решения, стратегии поведения или стратегии управления. Следовательно, возникает необходимость в построении таких специальных систем распознавания, чтобы обеспечивалась наибольшая эффективность системы управления, стоящей над системой распознавания. Это означает подчиненность цели системы распознавания целям MNP.

Вторая причина состоит в том, что эффективность системы распознавания в целом непосредственно зависит от эффективности инструментальных средств системы распознавания – программно реализованных алгоритмов построения описания классов объектов на языке признаков, обработки измерительной информации в целях определения признаков, собственно

распознавания, корректировки априорных описаний и т.д. Это в свою очередь означает подчиненность целей средств системы распознавания цели системы в целом.

Постановка задачи

Для целей структурирования задачи воспользуемся наиболее распространенной моделью распознавания образов - моделью классификации, состоящей из трех частей (уровней) — датчика, выделителя признаков и классификатора. Функции каждого из уровней таковы:

- датчик воспринимает воздействие и преобразует его к виду, удобному для машинной обработки;
- выделитель признаков выделяет из входных данных предположительно относящуюся к делу (релевантную) информацию;
- классификатор относит эти данные к одной из нескольких категорий.

С точки зрения эффективного разделения всех функций провести черту между этими тремя уровнями можно весьма условно. Так, идеальный выделитель признаков значительно упрощает работу классификатора, тогда как при наличии мощного классификатора не требуется ряд функций выделителя признаков. Разграничение функций уровней весьма важно, но делается оно, как правило, из практических, нежели теоретических соображений.

Функция выделения признаков более специализирована по сравнению с функцией классификации. Хороший выделитель признаков, предназначенный для одной цели, принесет, по-видимому, малую пользу при классификации других объектов. Однако большое число технических приемов было развито в связи с задачей извлечения полезной информации [2].

В работе предлагается способ реализации функции выделения признаков для классификации объекта, представляющего собой периодическую последовательность квантов гармонических колебаний.

Задача классификации по существу представляет собой задачу разбиения пространства признаков на области, по одной для каждого класса. Разбиение это надо производить так, чтобы не было ошибочных решений, а если этого сделать нельзя, то уменьшить вероятность ошибки. При этом задача классификации превращается в задачу статистической теории принятия решений, широко применяемую в различных областях теории распознавания образов [1,2].

Способы реализации функции классификации объекта, представляющего собой периодическую последовательность квантов гармонических колебаний, на основе априори выделенных в результате решения предыдущей задачи признаков, выходит за рамки настоящей статьи.

Основная часть

Реальные объекты обладают бесконечным числом признаков. С другой

стороны, классификация, производимая человеком, обычно основывается на небольшом числе признаков, как например, максимальная величина, основная частота и т. д. Каждое из этих измерений несет значительную информацию для целей классификации и выбирается в соответствии с физическим смыслом задачи.

Очевидно, что с уменьшением числа входных величин классификатора его проектирование упрощается. Для того чтобы добиться этого, следует наметить пути для выбора или извлечения существенных информативных признаков из всей совокупности наблюдаемых. Эту задачу называют задачей выбора информативных признаков, и она составляет другой важный раздел теории распознавания образов [3]. Выбор признаков можно рассматривать как отображение исходного n -мерного пространства в пространство меньшей размерности. При этом необходимо сохранить свойство разделимости распределений, соответствующих разным классам. Следовательно, отображение должно быть выполнено без существенной потери этого свойства.

Как уже было сказано, задача распознавания образов состоит из трех частей: съем информации (датчик) - выбор информативных признаков и собственно классификация (рис.1). Как уже было сказано выше, при проектировании системы распознавания удобнее разделить задачу распознавания именно на такие три части и изучать их независимо друг от друга.



Рис.1 Блок-схема системы распознавания образом

При реализации функции выделения признаков выбранного в данной работе объекта возникает задача представления модели данного объекта. Трафик (на интервале кванта) на физическом уровне в беспроводной компьютерной сети представляем модулируемым сигналом. Для учета данной особенности трафика

беспроводной компьютерной сети предлагается использовать классическое разложение Фурье.

Было разработано приложение, позволяющее представлять трафик компьютерной сети такого типа. Графический интерфейс данного приложения представлен на рис. 2.

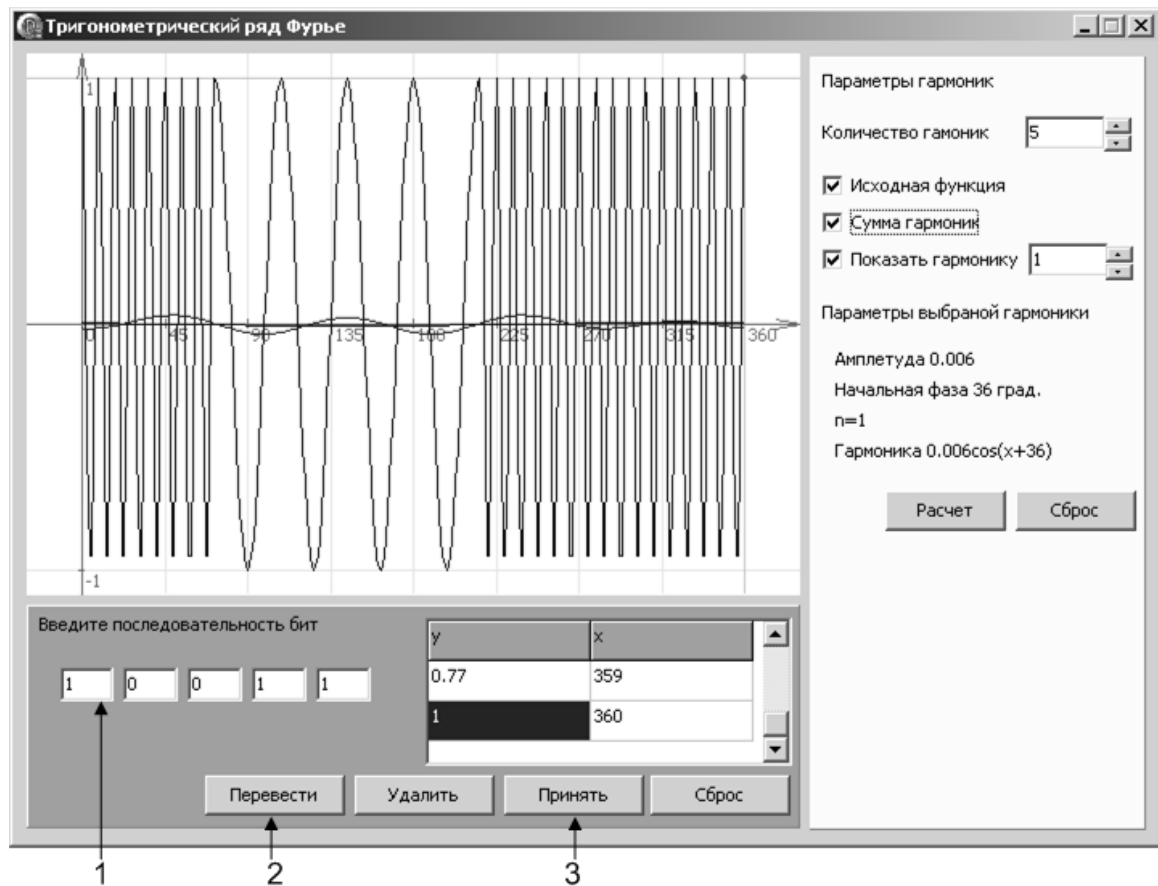


Рис. 2 Графический интерфейс приложения

На рис. 2 цифрой 1 обозначен элемент программы, используемый для ввода тестовой последовательности бит. Цифрой 2 обозначена кнопка «Принять», после нажатия которой вычисляются координаты последовательности точек моделирующего последовательность бит в беспроводной компьютерной сети. Для кодирования бит используется частотная модуляция.

Цифрой 3 обозначена кнопка «Принять», которая инициирует разложение в ряд Фурье, полученной ранее функции. При этом ряд Фурье, порожденный действительной функцией $f(t)$, для которой существует интеграл $\int_{-\pi}^{\pi} |f(t)| dt$, есть бесконечный тригонометрический ряд

$$\frac{1}{2}a_0 + \sum_{k=1}^{\infty} (a_k \cos kt + b_k \sin kt) \equiv \sum_{k=-\infty}^{\infty} c_k e^{ikt}$$

Коэффициенты которого определяются по формулам Эйлера-Фурье

$$\left. \begin{aligned} a_k &= \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \cos kt \, dt, \quad b_k = \frac{1}{\pi} \int_{-\pi}^{\pi} f(t) \sin kt \, dt, \\ c_k = \bar{c}_{-k} &= \frac{1}{2} (a_k - ib_k) = \frac{1}{2\pi} \int_{-\pi}^{\pi} f(t) e^{-ikt} \, dt \end{aligned} \right\} (k = 0, 1, 2, \dots).$$

В разделе «Параметры гармоник» задается количество гармоник и управление отображаемыми данными на графике для уменьшения загруженности. В разделе «Параметры выбранной гармоники» отображаются данные для последующей классификации. Этими параметрами, очевидно, будут являться такие параметры функции как амплитуда, частота и фаза.

Выводы

Разработанное приложение позволяет реализовывать функцию выделения признаков трафика в беспроводной сети на основе классического разложения Фурье.

Следующим этапом исследования способов распознавания трафика в беспроводной компьютерной сети является анализ наиболее информативных признаков с целью последующей классификации распознаваемого объекта с определением эффективного критерия качества.

Литература

1. Я. З. Цыпкин, Информационная теория идентификации. — М.: Наука. Физматлит, 1995. — 336 с.
2. О. И. Ларичев Теория и методы принятия решений: Учебник. — М.: Логос, 2000. — 296 с.: ил.
3. Тоценко В. Г. Методы и системы поддержки принятия решений. Алгоритмический аспект / Тоценко В. Г. — К.: Наукова думка, 2002. — 381 с.
4. Тригонометрический ряд Фурье. Реализация в Delphi вывода данных и графика Excel. <http://www.deamolit.ru/index.php/delphi/26--delphi-excel.html>