УДК 65.012.8: 621.395

В.И. Корниенко, А.В. Герасина

ГВУЗ «Национальный горный университет», Днепропетровск

ЛИНЕЙНОЕ ПРЕДСКАЗАНИЕ В СИСТЕМЕ КОНФИДЕНЦИАЛЬНОЙ ТЕЛЕФОННОЙ СВЯЗИ ПО АТМ-СЕТИ

Исследованы алгоритмы линейного предсказания речевых сигналов с помощью адаптивного фильтра с конечной импульсной характеристикой. Путем моделирования оценена точность предсказания адаптивного фильтра в системе конфиденциальной телефонной связи по АТМ-сети.

Ключевые слова: *конфиденциальная связь, АТМ-сеть, линейное предсказание, адаптивный фильтр.*

Введение

Обеспечение телефонной конфиденциальной связи является одной из важных задач защиты информации в телекоммуникациях.

В настоящее время распространение среди операторов телефонной связи получила технология асинхронной передачи данных в сетях АТМ [1]. При этом между пользователями организуется виртуальный канал, который действует до момента окончания передачи.

Ячейки АТМ имеют фиксированную длину и следуют друг за другом без перерывов, что облегчает процедуры обработки сигнала и позволяет повысить скорость передачи информации.

Постановка задачи. Использование для конфиденциальной телефонной связи сетей с асинхронной передачей АТМ ставит вопрос о к качестве телефонной связи при ограниченной пропускной способности сети, использовании каналов связи невысокого качества и обеспечении конфиденциальности от абонента до абонента. Снижение качества телефонной связи в АТМ-сети происходит из-за потерь ячеек, возникающих при необратимых искажениях заголовков или перегрузках коммутаторов. Так как речевой сигнал (РС) обладает высокой избыточностью, то на периоде локальной стационарности возможно осуществить его восстановление с минимальными искажениями.

Одним из путей восстановления РС в тракте приема является механизм линейного предсказания ячеек АТМ, потерянных при передаче в сети.

Цель статьи. Исследование алгоритмов линейного предсказания речевых сигналов, а также оценка эффективности их использования в системе конфиденциальной телефонной связи по АТМ-сети.

Система конфиденциальной связи

Система связи (рис. 1) ориентирована на передачу от абонента до абонента конфиденциального телефонного трафика с изменяющейся скоростью и подавлением пауз [1].

При сжатии речи для подавления пауз используется идентификатор типа полезной нагрузки заголовка ячейки АТМ. Он принимает разные значения в зависимости от наличия в передаваемых ячейках активных фрагментов речи.

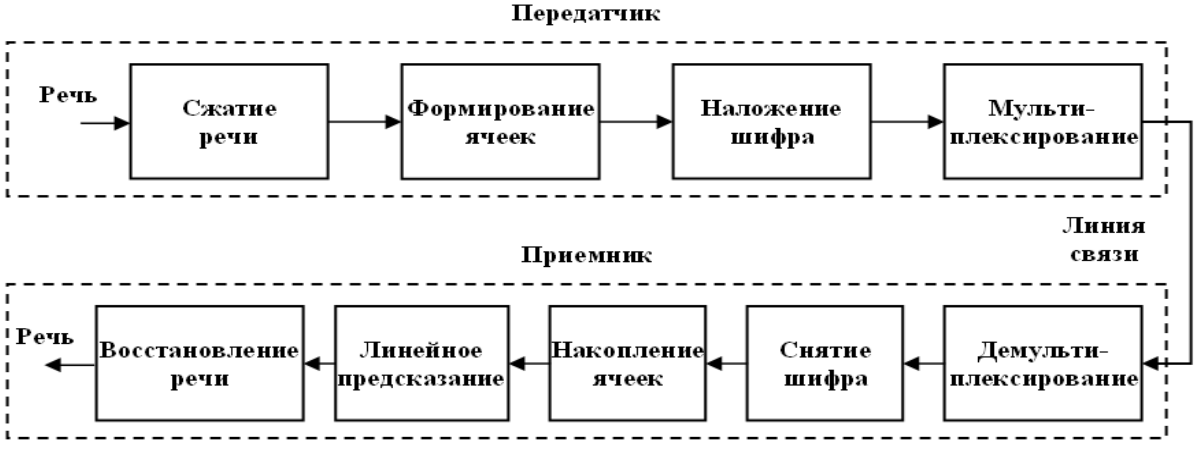


Рис. 1. Схема системы конфиденциальной связи

Далее в тракте передачи осуществляется преобразование аналогового РС в цифровую форму и формирование ячеек АТМ.

Ячейки, содержащие паузы речевой активности, не шифруются и не передаются, что уменьшает общую нагрузку на сеть.

Для обеспечения криптографической стойкости выполняется шифрование данных по методу гаммирования. При этом, на этапе установления соединения формируется начальное заполнение шифратора с выполнением требований по стохастичности, равномерности и некоррелируемости. При шифровании цифровой РС суммируется с двоичной псевдослучайной последовательностью.

Сформированные и зашифрованные данные с помощью мультиплексора передаются в линию связи. При отсутствии ячеек для передачи с целью поддержания синхронизма мультиплексор осуществляет вставку в выходной сигнал пустых ячеек.

В приемнике демультиплексор выполняет функции, обратные мультиплексору, включая исправление ошибок в заголовках ячеек АТМ. В случае невозможности исправления ошибок, принятая ячейка дальнейшей обработке не подлежит (считается потерянной).

Пакетное дешифрование осуществляется по алгоритму, аналогичному для наложения шифра в передатчике.

Далее накапливаются ячейки и выполняется выравнивание задержек с целью компенсации дисперсии времени доставки ячеек АТМ в сети.

Линейное предсказание ячеек, потерянных при передаче в сети, осуществляется на периоде локальной стационарности РС синхронно со скоростью передачи. При этом в качестве исходных данных для предсказания используется информация из принятых ранее блоков данных.

Полученный цифровой РС с заполненными паузами и восстановленными ячейками синхронно подается на синтезатор, где осуществляется восстановление речи путем преобразования сигнала в аналоговую форму.

Алгоритмы линейного предсказания речи

Спектр кратковременного РС имеет глобальный максимум в окрестности от 300 до 800 Гц и убывает со скоростью от 6 до 12 дБ/октаву [2], а медленно меняющаяся автокорреляционная функция РС свидетельствует о достаточно тесной связи между отсчетами сигнала.

Значение корреляции для типичного единичного выборочного значения составляет 0,79…0,87, а интервал корреляции имеет длительность 4…6 отсчетов [2].

Поскольку разность между соседними временными отсчетами для речи мала, то кодирование РС базируется на передаче от выборки к выборке разностей их значений, что реализуется N-отводными линейными кодерами с предсказанием [3].

Контур предсказания описывается как:

$$\varepsilon(k) = x(k) - \bar{x}(k),$$

где $x(k)$ – k-я выборка; $\bar{x}(k)$ – предсказанное значение выборки; $\varepsilon(k)$ – ошибка предсказания.

Кодер корректирует свои предсказания, составляя сумму предсказанного значения и ошибки предсказания. Контур корреляции описывается как:

$$\bar{\varepsilon}(k) = \text{quant}\left[\varepsilon(k)\right], \quad \bar{x}(k) = \hat{x}(k) + \bar{\varepsilon}(k),$$

где $\text{quant}(\ )$ – операция квантования, $\hat{x}(k)$ – оценка входной выборки.

Тогда предсказание примет следующий вид:

$$x(k \mid k-1) = a_1 x(k-1) + a_2 x(k-2) + ... + a_N x(k-N).$$

Среднеквадратическая ошибка предсказания равна:

$$E\{\varepsilon(k)\varepsilon(k)\} = E\left\{\left[x(k) - x(k \mid k-1)\right]^2\right\}.$$

По существу N-отводные линейные кодеры с предсказанием реализуются на основе адаптивных линейных прогнозирующих фильтров (ПФ) с конечной импульсной характеристикой (КИХ) [3]. В них процесс адаптации включает оценивание искомого выхода фильтра и корректировку его коэффициентов по значению выходной ошибки (рис. 2).

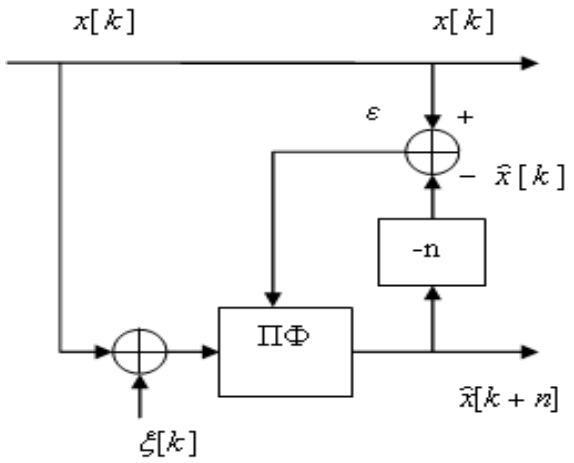


Рис. 2. Схема адаптации ПФ

Тут задержка и прогноз на n тактов обозначены как $-n$ и $+n$, а $\xi[k]$ – шум.

В процессе работы ПФ на каждом такте по величине ошибки $\varepsilon[k] = x[k] + \bar{x}[k]$ между фактическим $x[k]$ и прогнозируемым $\bar{x}[k]$ значениями сигнала осуществляется адаптация коэффициентов ПФ.

Разностное уравнение линейного ПФ с КИХ имеет вид:

$$\hat{x}[k+n] = \sum_{r=0}^{N} a_r \cdot x[k-r],$$

где a_r, N – коэффициенты фильтра и его порядок, соответственно.

ПФ с КИХ обладают асимптотической устойчивостью и линейной фазо-частотной характеристикой.

Моделирование блока линейного предсказания

Целью моделирования был выбор порядка (M) ПФ и значения коэффициента скорости его обучения (μ) в условиях шума (nvar) и требуемой (желаемой) ошибке предсказания ($\overline{\varepsilon_{\text{ÒÐ}}}$).

Программа моделирования включала определение значения ошибки предсказания $\bar{\varepsilon}$ для уровня шума $nvar = 0,5$, различных порядков адаптивного фильтра $M = \{16,\ 32,\ 64,\ 128\}$ и для различных значений коэффициента скорости обучения $\mu = \{0,25,\ 0,50,\ 0,75\}$.

Моделирование выполнялось в среде Matlab с помощью пакета программ Filter Designer. В качестве тестового речевого сигнала использовалась сумма гармоник с частотой 400, 1000 и 3000 Гц длительностью $T = 22,5$ ì ñ (период стационарности речевого сигнала).

Соответственно количество отсчетов сигнала с частотой дискретизации $F_D = 8$ кГц соответственно $N = T \cdot F_D = 180$.

В результате моделирования определены значения средней ошибки $\bar{\varepsilon}$ при уровне помех $nvar = 0,5$, которые приведены в табл. 1 и на рис. 3.

Таблица 1

Значения средней ошибки

μ \ M	16	32	64	128
0,25	0,457	0,160	0,090	0,050
0,50	0,210	0,076	0,047	0,035
0,75	0,110	0,013	0,007	0,004

Если задаться допустимым уровнем ошибки $\bar{\varepsilon}_{\text{ÒÐ}} \le 0,05\ (5\%)$, то по табл. 1 и рис. 3 получим, что порядка фильтра должен быть M=32 и значение коэффициента скорости обучения $\mu = 0,75$ (ошибка $\bar{\varepsilon} = 0,013$) или M=64 и $\mu = 0,5$ ($\bar{\varepsilon} = 0,047$), или M=128 и $\mu = 0,25$ ($\bar{\varepsilon} = 0,05$).

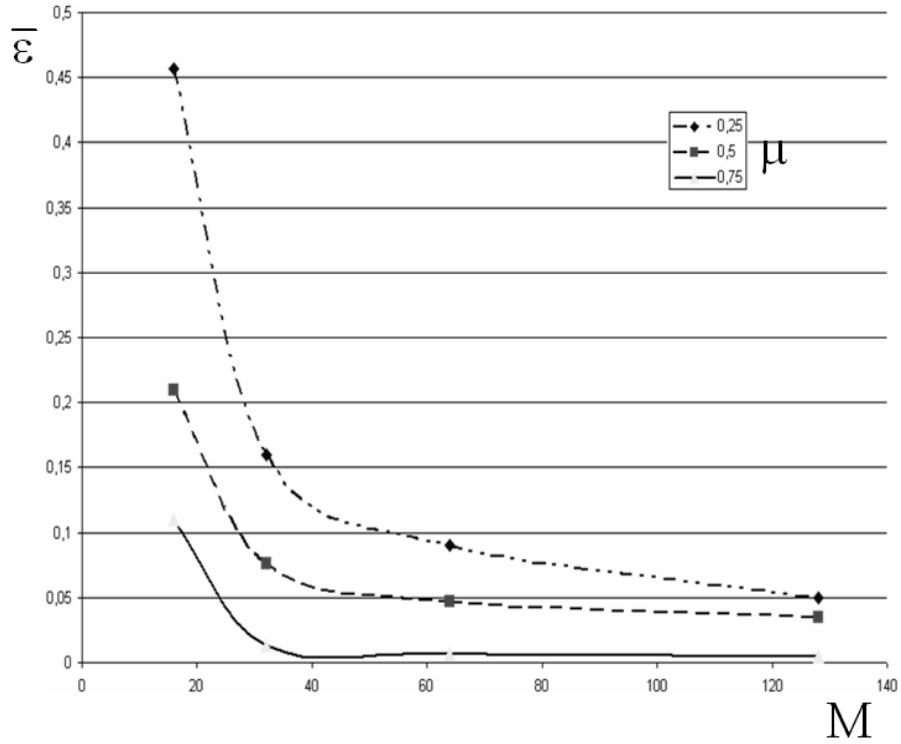
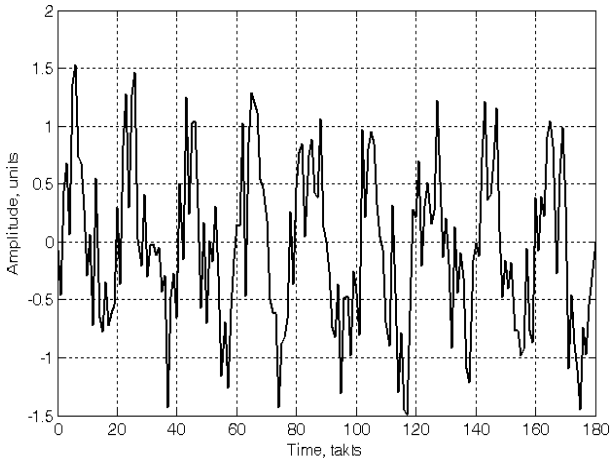
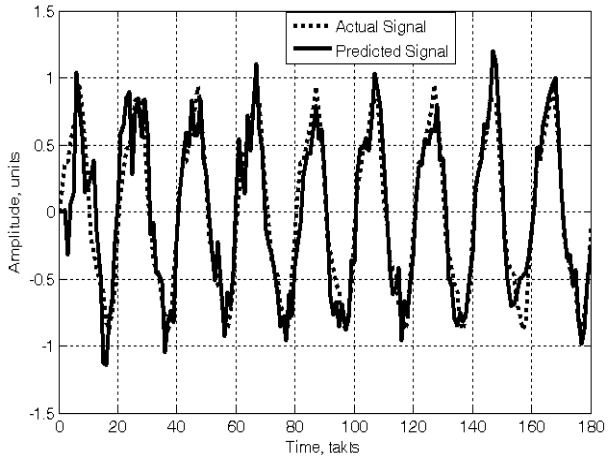


Рис. 3. Значения средней ошибки предсказания

Примем значения порядка M=32 и коэффициента $\mu = 0,75$, поскольку соответствующее значение ошибки $\bar{\varepsilon} = 0,013 < \bar{\varepsilon}_{\text{ÒÐ}}$ и порядок ПФ наименьший, что обеспечивает сокращение вычислений и удешевлению аппаратной реализации системы. Для выбранных условий графики сигналов имеют вид, представленный на рис. 4, а автокорреляционная функция ошибки приведена на рис. 5.



а



б

Рис. 4. Входной сигнал с шумом (а) и его предсказанное значение (б)

Выводы

Повышение эффективности системы конфиденциальной связи достигается путем включения в приемник блока линейного предсказания потерянных ячеек АТМ в телефонных сетях с низкой пропускной способностью.

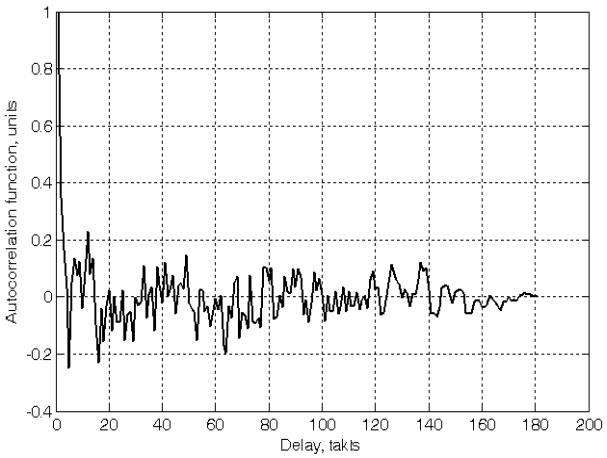


Рис. 5. Автокорреляционная функция ошибки предсказания

Установлено, что линейная адаптивная фильтрация обеспечивает ошибку предсказания зашумленного речевого сигнала с точностью:

– не хуже 5 % для порядка фильтра M=24;

– не хуже 1,3 % для порядка фильтра M=32.

Дальнейшие исследования должны быть направлены на техническую реализацию предложенных решений.

Список литературы

1. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К.: Юниор, 2003. – 496 с.

2. Беллами Дж. Цифровая телефония: Пер. с англ. / Дж. Беллами. – М.: Эко-Тренд, 2004. – 640 с.

3. Адаптивные фильтры: Пер. с англ. / Под ред. К.Ф.Н. Коуэна и П.М. Гранта. – М.: Мир, 1988. – 392 с.

Поступила в редколлегию 18.12.2012

Рецензент: д-р техн. наук, проф. М.А. Алексеев, ГВУЗ «Национальный горный университет», Днепропетровск.

ЛІНІЙНИЙ ПРОГНОЗ В СИСТЕМІ КОНФІДЕНЦІЙНОГО ТЕЛЕФОННОГО ЗВ'ЯЗКУ ПО АТМ-МЕРЕЖІ

В.І. Корнієнко, О.В. Герасіна

Досліджені алгоритми лінійного прогнозу мовних сигналів за допомогою адаптивного фільтру з кінцевою імпульсною характеристикою. Шляхом моделювання оцінена точність прогнозу адаптивного фільтру в системі конфіденційного телефонного зв'язку по АТМ-мережі.

Ключові слова: *конфіденційний зв'язок, АТМ-мережа, лінійний прогноз, адаптивний фільтр.*

LINEAR PREDICTION IN CONFIDENTIAL TELEPHONE COMMUNICATION ON ATM-NETWORK

V.I. Korniyenko, A.V. Gerasina

The algorithms of linear prediction of voice signals are investigational by an adaptive filter with eventual impulsive description. By a simulate estimation of exact prediction of adaptive filter is appraised in a confidential telephone communication on ATM-network.

Keywords: *confidential connection, ATM-network, linear prediction, adaptive filter.*