ДОКЛАДЫ БГУИР

Выходит два раза в квартал

Научный журнал издается с января 2003 года

АДРЕС РЕДАКЦИИ:

220013, Минск, ул. П. Бровки, 6, к. 327

293 88 41

www.doklady.bsuir.by

doklady@bsuir.by

СОДЕРЖАНИЕ

ИНФОРМАТИКА

КРАТКИЕ СООБЩЕНИЯ

Учредитель: Учреждение образования
"Белорусский государственный университет информатики и радиоэлектроники"

Редактор Т.В. МИРОНЕНКО
Компьютерная дизайн и верстка Е.Г. МАКЕЙЧИК

Подписано в печать 11.05.2009. Формат 60×84 ⅛. Гарнитура "Таймс".
Печать ризографическая. Усл. печ. л. 15,35. Уч. изд. л. 13,5. Тираж 125 экз. Заказ 232.
Индекс для индивидуальной подписки 00787. Подписная цена 15 060 р.
Индекс для ведомственной подписки 007872. Подписная цена 15 131 р.

Отпечатано в БГУИР.
Лицензия ЛП №02330/0494175 от 03.04.2009. 220013, г. Минск, ул. П. Бровки, 6

Издатель: Учреждение образования "Белорусский государственный университет информатики и радиоэлектроники".
Свидетельство № 1954 от 28.03.2008.

DOKLADY BGUIR

Published twice quarterly

The journal has been published since January, 2003

Editor-In-Chief MP. Batura

ADDRESS OF EDITORIAL OFFICE

220013, Minsk, P. Brovka Str., 6, Room 327

293 88 41

www.doklady.bsuir.by

doklady@bsuir.by

CONTENTS

INFORMATICS

SHORT NOTES

ИНФОРМАТИКА

УДК 621.391

ОБЪЕКТНОЕ ПРЕДСКАЗАНИЕ ИЗМЕНЕНИЯ ВИДЕОДАННЫХ ПРИ ГОРИЗОНТАЛЬНОМ ПЕРЕМЕЩЕНИИ КАМЕРЫ

Т.М. АЛЬ-ДЖУБУРИ, В.Ю. ЦВЕТКОВ, В.К. КОНОПЕЛЬКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 5 октября 2009

Предложен метод объектного предсказания изменения видеоданных на основе модели движения камеры. Суть метода состоит в объектной декомпозиции опорного кадра видеоданных, классификации объектов по дальности, расслоении опорного кадра по дальности и формировании нового кадра на основе модели движения камеры, учитывающей смещения объектов навстречу вектору движения камеры. Метод обеспечивает уменьшение ошибки предсказания изменения видеоданных при движении камеры за счет использования информации о характеристиках, условиях установки и параметрах движения камеры.

Ключевые слова: модель движения камеры, объектная декомпозиция изображения, предсказание изменения видеоданных.

Введение

В связи с ростом объемов передаваемых и хранимых видеоданных актуальна проблема их компактного представления. Эффективными способами решения данной проблемы являются сжатие видеоданных с устранением межкадровой избыточности на основе компенсации движения и частичное или полное замещение естественных видеоданных псевдореалистическими, синтезированными на основе естественных, но требующими существенно меньших ресурсов при передаче и хранении. Эти подходы используются в стандартах сжатия видео MPEG-2, MPEG-4 и H.264 [1], технологии MPEG-7 [2], а также методах формирования трехмерных панорамных [3] и псевдостереоскопических [4] изображений. Эффективность данных подходов ограничена отсутствием предсказания изменения видеоданных при перемещении камеры, для реализации которого необходима информация о характеристиках, условиях установки и параметрах движения камеры. В общем случае получение данной информации проблематично. Однако, существует ряд систем, для которых данная проблема может быть решена. Примерами могут служить системы видеонаблюдения с несколькими стационарно установленными камерами, а также одной или несколькими перемещающимися камерами. В этих случаях возможно предсказание изменения видеоданных при перемещении камеры или при переключении между стационарными камерами с перекрывающимися областями видимости по известным значениям угла видимости, высоты установки, угла наклона и направления перемещения камеры.

Цель данной работы – разработать метод предсказания изменения видеоданных на основе модели движения камеры.

Модель движения камеры

В общем случае модель M_C движения видеокамеры может быть задана следующим набором параметров:

$$M_C = \|D_Y, D_U, D_V, Y, X, \alpha_Y, \alpha_X, A, H, S_X, S_Z, \beta_Z, \beta_Y, \beta_X\|, \quad (1)$$

где D_Y, D_U, D_V – битовая глубина формируемого камерой цветного изображения для яркостной и двух цветоразностных компонент; Y, X – размеры формируемого камерой изображения по вертикали и горизонтали; $t = \overline{0, T-1}$ – дискреты времени, совпадающие с номерами кадров, формируемых камерой; T – период дискретного времени моделирования движения камеры; α_Y, α_X – углы обзора камеры по вертикали и горизонтали; $A = \|a(y, x, t)\|_{y=\overline{0,Y-1}, x=\overline{0,X-1}}$ – матрица корректирующих коэффициентов, учитывающих аберрации оптической системы камеры для каждого пикселя формируемого изображения; H – высота установки камеры; S_X, S_Z – смещения камеры в горизонтальной плоскости перпендикулярно и вдоль оптической оси относительно предыдущего положения камеры ($S_X = 0$, $S_Z = 0$); β_Z – угол наклона нижней границы изображения к поверхности (угол крена камеры); β_Y – угол поворота оптической оси камеры в горизонтальной плоскости относительно предыдущего положения камеры ($\beta_Y = 0$); β_X – угол наклона оптической оси камеры к поверхности ($\beta_X > 0$, если оптическая направлена вверх и $\beta_X < 0$, если оптическая ось направлена вниз).

Параметры $H, S_X, S_Z, \beta_Z, \beta_Y, \beta_X$ при $t = \overline{0, T-1}$ определяют траекторию движения камеры.

С учетом конкретных условий применения модель движения камеры может быть существенно упрощена. Частным, но важным случаем является горизонтальное движение ($S_Z = 0$, $\beta_Y = 0$, $H = const$) камеры, формирующей полутоновое изображение ($D_Y = 8$, $D_U = 0$, $D_V = 0$). Если предсказание основано на одном исходном кадре и распространяется только на один последующий кадр, то $T = 2$. Учитывая особенности построения ряда систем видеонаблюдения, при $T = 2$ модель подвижной камеры может быть упрощена за счет следующих дополнительных ограничений: $\alpha_Y = const$, $\alpha_X = const$ (постоянное фокусное расстояние); $a(y, x, t) = 1$ (оптическая система описывается моделью тонкой линзы); $\beta_X = const$ (постоянный угол наклона оптической оси камеры); $\beta_Z = 0$ (отсутствие крена). В результате упрощенная модель подвижной камеры представляется следующим выражением:

$$M_C = \|Y, X, \alpha_Y, \alpha_X, H, S_X, \beta_X\|. \quad (2)$$

В данной модели траектория движения камеры задается единственным параметром S_X.

Описание метода

Предлагается метод объектного предсказания изменения видеоданных при перемещении камеры на основе модели M_C движения камеры, использующий опорный кадр $C_G = \|c_G(y, x)\|_{y=\overline{0,Y-1}, x=\overline{0,X-1}}$ видеоданных, соответствующий исходному положению камеры, а также информацию о характеристиках, параметрах установки и перемещения камеры для формирования кадров $\hat{C}_G = \|\hat{c}_G(y, x, t)\|_{y=\overline{0,Y-1}, x=\overline{0,X-1}, t=\overline{1,T-1}}$, соответствующих положениям камеры в дискретные моменты времени на периоде T. Метод описывается следующим выражением

$$\hat{C}_G = f_{OP}(C_G, M_C), \quad (3)$$

где f_{OP} – функция объектного предсказания изменения видеоданных.

Основными шагами метода являются объектная декомпозиция опорного кадра видеоданных (формируется информация о количестве и расположении объектов опорного кадра), классификация объектов по дальности (каждый объект причисляется к некоторому классу объектов по дальности в зависимости от его удаленности от камеры), расслоение опорного кадра видеоданных по дальности (определяются расстояния до равноудаленных от камеры объектов, группируемых в слои изображения по дальности), формирование нового кадра видеоданных (объекты и фон опорного кадра смещаются с учетом вектора движения камеры и интерполируются значения образующихся неопределенных пикселей, заслоненных объектами на опорном кадре).

Для эффективного использования метода объекты опорного кадра должны иметь высокий контраст по отношению к фону и располагаться на ровной поверхности, достаточно хорошо аппроксимирующейся плоскостью. Несмотря на данные ограничения, сужающие область применения предлагаемого метода, он может достаточно эффективно использоваться для сжатия видеоданных с предсказанием движения камеры в системах видеонаблюдения помещений, открытых участков равнинной местности и поверхностей водоемов. Кроме того, возможно использование данного метода в этих условиях для формирования второго изображения псевдостереопары, а также последовательности кадров синтетического видео.

В случае простой структуры опорного кадра, содержащего высококонтрастные по отношению к однородному фону и низкоконтрастные по отношению друг к другу объекты, не заслоняющие частично или полностью другие объекты, отдельные шаги метода могут быть существенно упрощены. При использовании в этом случае упрощенной модели движения камеры, представленной выражением (2), метод описывается соотношением

$$\hat{C}_G = f_{OP}(C_G, M_C) \quad (4)$$

и сводится к следующим четырем шагам.

1) Объектная декомпозиция опорного кадра C_G видеоданных. На данном шаге осуществляется бинаризация опорного кадра видеоданных и формируется матрица объектной декомпозиции, содержащая информацию о количестве и расположении изолированных объектов опорного кадра, которые представляют собой совокупности единичных пикселей, разделенные друг от друга нулями. Результатом выполнения данного шага являются количество N_O изолированных объектов в опорном кадре видеоданных и матрица $M_D = \|m_D(y,x)\|_{y=\overline{0,Y-1},\,x=\overline{0,X-1}}$ объектной декомпозиции опорного кадра видеоданных.

2) Классификация объектов опорного кадра видеоданных по дальности. Формируется вектор классификации объектов по дальности, с помощью которого каждый изолированный объект, выделенный в матрице объектно-ориентированной декомпозиции, причисляется к некоторому классу объектов по дальности в зависимости от минимального значения y-координат пикселей, образующих данный объект. Результатом выполнения данного шага является вектор $D_Y = \|d_Y(i)\|_{i=\overline{0,N_O-1}}$ классификации объектов по дальности, значение каждого i-го элемента $d_Y(i) \in [0, Y-1]$ которого определяет класс соответствующего i-го объекта по дальности. Класс характеризует удаленность объекта от камеры. Чем меньше значение $d_Y(i)$, тем ближе к камере расположен i-й объект. Максимальное число различных классов равно $Y+1$ – на один больше числа пикселей в кадре по вертикали. К классу Y принадлежат пиксели, не принадлежащие ни одному из N_O объектов.

3) Расслоение опорного кадра видеоданных по дальности. Оно основано на использовании параметров Y, α_Y, H и β_X модели движения камеры для представления опорного кадра видеоданных в виде бинарной проекции трехмерной сцены, расстояние до каждого объекта которой оценивается по смещению проекции точки местоположения объекта от нижней границы кадра. В результате выполнения данного расслоения формируется вектор $D_Z = \|d_Z(y)\|_{y=\overline{0,Y-1}}$ расстояний от камеры до объектов, значение каждого y-го элемента $d_Z(y) \in [0, \infty)$ которого определяет расстояние от камеры до объектов y-го слоя, смещенных на y пикселей от нижнего края опорного кадра видеоданных. Расстояния определяются в тех единицах измерения, которые использовались для определения параметра H модели движения камеры.

4) Формирование нового кадра $\hat{C}_G$ видеоданных. Объекты каждого слоя опорного кадра видеоданных сдвигаются на некоторое число пикселей в зависимости от удаленности слоя от камеры. Значения пикселей, заслоненных объектами на опорном кадре, устанавливается равным среднему значению яркости фона.

Формирование нового кадра видеоданных

Предлагается алгоритм формирования по опорному кадру видеоданных, соответствующему исходному положению камеры, нового кадра, соответствующего горизонтальному смещению камеры относительно исходного положения. Алгоритм основан на модели движения камеры и предположении, что при перемещении камеры расстояния от камеры до объектов не изменяются (или, по крайней мере, эти изменения не могут быть отображены на новом кадре видеоданных из-за недостаточной разрешающей способности фотоприемной матрицы камеры). Такое предположение возможно, если выполняется следующее условие

$$\sqrt{d_Z(x)^2 + S_X^2} - d_Z(x) \le d_Z(x) - d_Z(x). \quad (5)$$

Условие (5) имеет место во многих практических случаях, в том числе в системах видеонаблюдения.

Алгоритм формирования нового кадра видеоданных состоит из следующих шагов.

1) Инициализация вектора $S_D = \|s_D(y)\|_{y=\overline{0,Y-1}}$ смещений слоев опорного кадра

$$s_D(y) = 0 \quad (6)$$

при $y = \overline{0,Y-1}$.

2) Инициализация матрицы $M_S = \|m_S(y,x)\|_{y=\overline{0,Y-1},\, x=\overline{0,X-1}}$ смещенных пикселей опорного кадра видеоданных

$$m_S(y,x) = 0 \quad (7)$$

при $y = \overline{0,Y-1}$ и $x = \overline{0,X-1}$.

3) Определение горизонтального виртуального фокуса F_X модели оптической системы камеры

$$F_X = (X/2)\,/\,tg\left(\alpha_X/2\right). \quad (8)$$

4) Определение средней яркости $\bar{c}_G$ фона опорного кадра видеоданных

$$\bar{c}_G = \left(\sum_{y=0}^{Y-1}\sum_{x=0}^{X-1}(c_G(y,x)\cdot(1-c_B(y,x)))\right) \Big/ \left(Y\cdot X - \sum_{y=0}^{Y-1}\sum_{x=0}^{X-1}c_B(y,x)\right). \quad (9)$$

5) Цикл определения величин смещений слоев опорного кадра видеоданных. Для каждого элемента вектора D_Z расстояний до объектов рассчитывается значение соответствующего элемента вектора S_D с помощью выражения

$$s_D(y) = \left\lfloor F_X \cdot \frac{S_X}{\sqrt{d_Z(y)^2 - S_X^2}} \right\rfloor \quad (10)$$

при $y = \overline{0,Y-1}$,

где $\lfloor$ – операция округления до ближайшего целого.

6) Цикл смещения слоев опорного кадра видеоданных. Операция смещения слоев применяется к строкам опорного кадра видеоданных в направлении сверху вниз. При смещении камеры вправо ($S_X > 0$) операция смещения применяется к пикселям каждой строки в направлении слева направо. При смещении камеры влево ($S_X < 0$) операция смещения применяется к пикселям каждой строки в направлении справа налево.

Для пикселей $c_G(y,x)$ опорного кадра C_G видеоданных, не отмеченных в матрице M_D объектной декомпозиции ($m_D(y,x) = 0$ – т.е. пиксель не принадлежит ни одному из N_O объектов), смещение осуществляется на величину $s_D(y)$ при условии, что пиксель $\tilde{c}_G(y, x - s_D(y))$ формируемого кадра $\tilde{C}_G$ видеоданных является неопределенным и находится в пределах кадра ($0 \le (x - s_D(y)) \le X$)

$$(m_S(y,x')=0)\rightarrow(c_G(y,x')=c_G(y,x)) \tag{11}$$

при $y=\overline{0,Y-1}$ и $x=\overline{0,X-1}$,

где $x'=x-s_D(y)$ – координата пикселя формируемого кадра видеоданных.

Для пикселей $c_G(y,x)$ опорного кадра C_G видеоданных, отмеченных в матрице M_D объектной декомпозиции ($m_D(y,x)\neq 0$ – т.е. пиксель принадлежит одному из N_O объектов), смещение осуществляется на величину $s_D(d_Y(m_D(y,x)))$ при условии, что пиксель $\hat{c}_G(y,x-s_D(d_Y(m_D(y,x))))$ формируемого кадра $\hat{C}_G$ видеоданных не принадлежит более приближенному к камере объекту и находится в пределах кадра ($0\le x-s_D(d_Y(m_D(y,x)))<X$)

$$\begin{cases}(m_S(y,x'')=0)\rightarrow(\hat{c}_G(y,x'')=c_G(y,x)\wedge(m_S(y,x'')=m_D(y,x)))\\(m_S(y,x'')\neq 0)\rightarrow\left(\begin{array}{l}(d_Y(m_D(y,x))\le d_Y(m_S(y,x'')))\rightarrow\\\rightarrow(\hat{c}_G(y,x'')=c_G(y,x)\wedge(m_S(y,x'')=m_D(y,x)))\end{array}\right)\end{cases}. \tag{12}$$

при $y=\overline{0,Y-1}$ и $x=\overline{0,X-1}$,

где $x''=x-s_D(d_Y(m_D(y,x)))$ – координата пикселя формируемого кадра видеоданных.

7) Цикл поиска и определения значений пикселей формируемого кадра видеоданных, заслоненных объектами на опорном кадре. Значения пикселей, заслоненных объектами на опорном кадре, устанавливаются равным среднему значению яркости фона в соответствии с выражением

$$(m_S(y,x)=0)\rightarrow(\hat{c}_G=\bar{c}_G) \tag{13}$$

при $y=\overline{0,Y-1}$ и $x=\overline{0,X-1}$.

По окончанию цикла поиска и определения значений пикселей формируемого кадра видеоданных осуществляется выход из алгоритма.

В результате выполнения данного алгоритма формируется кадр $\hat{C}_G$ видеоданных, соответствующий новому положению камеры при ее горизонтальном перемещении на S_X относительно исходного положения в плоскости, параллельной плоскости изображения.

Оценка эффективности метода объектного предсказания изменения видеоданных

Для оценки эффективности разработанного метода объектного предсказания изменения видеоданных получены 5 полутоновых изображений тестовой трехмерной сцены – исходный видеокадр (рис. 1) и 4 видеокадра (рис. 2, *а – г*), соответствующие горизонтальному смещению камеры вправо на 1, 2, 3 и 4 см. Изображения получены с помощью цифровой камеры Sony Cyber-shot с отключенной автофокусировкой, установленной на высоте $H=10$ см и обеспечивающей размеры изображения по вертикали $Y=480$ и горизонтали $X=640$, углы видимости по вертикали $\alpha_Y=22.5^\circ$ и горизонтали $\alpha_X=50.2^\circ$, угол наклона оптической оси камеры к поверхности $\beta_X=-6^\circ$.

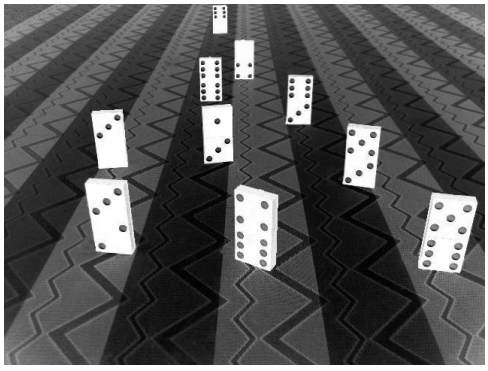
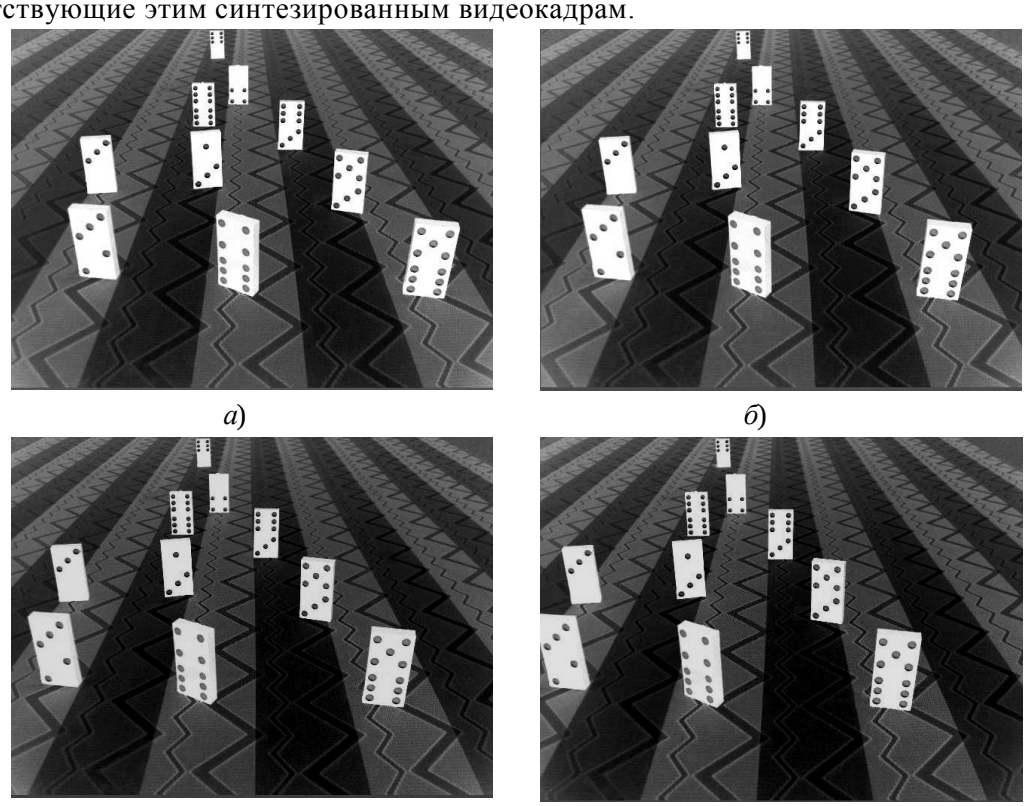


Рис. 1. Исходный видеокадр

На рис. 3 представлены видеокадры при смещении камеры вправо по горизонтали на $S_X = 1$см, $S_X = 2$см, $S_X = 3$см и $S_X = 4$см, синтезированные с помощью разработанного метода объектного предсказания изменения видеоданных и форматированные по горизонтали для удаления области неопределенности, возникающей справа при смещении камеры. На рис. 4 представлены образы ошибок предсказания, соответствующие этим синтезированным видеокадрам.



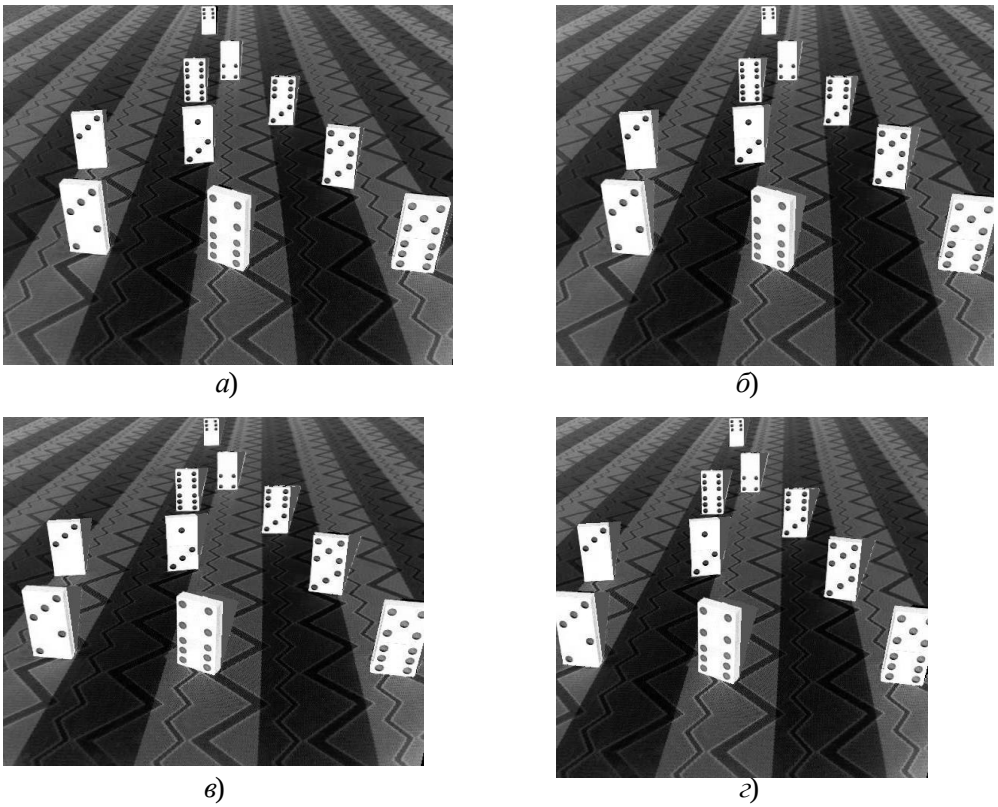
а) *б*) *в*) *г*)

Рис. 2. Полутоновые изображения тестовой трехмерной сцены:
а – видеокадр при $S_X = 1$ см; *б* – видеокадр при $S_X = 2$ см;
в – видеокадр при $S_X = 3$ см; *г* – видеокадр при $S_X = 4$ см

Для количественной оценки ошибки предсказания изменения видеоданных при движении камеры использована среднеквадратическая ошибка MSE, вычисляемая с помощью выражения

$$\mathrm{MSE} = \frac{\sum_{y=0}^{Y-1}\sum_{x=0}^{X'-1}\left(\quad\right)^2}{Y\,X'}, \qquad (14)$$

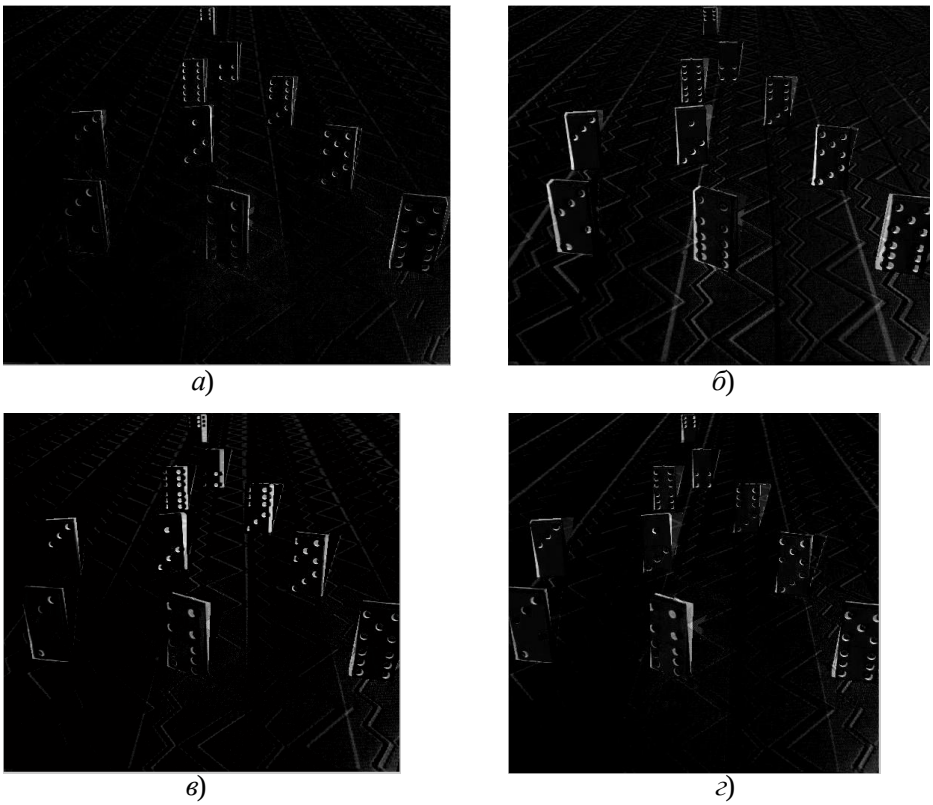
где X' – размер форматированного видеокадра по горизонтали с учетом удаления области неопределенности, возникающей при смещении камеры.



а) *б*)

в) *г*)

Рис. 3. Синтезированные полутоновые изображения тестовой трехмерной сцены:
а – видеокадр при $S_X = 1$ см; *б* – видеокадр при $S_X = 2$ см;
в– видеокадр при $S_X = 3$ см; *г*– видеокадр при $S_X = 4$ см



а) *б*)

в) *г*)

Рис. 4. Образы ошибок синтезированных полутоновых изображений тестовой трехмерной сцены:
а – образ ошибки при $S_X = 1$ см; *б* – образ ошибки при $S_X = 2$ см;
в – образ ошибки при $S_X = 3$ см; *г* – образ ошибки при $S_X = 4$ см

В таблице приведены значения среднеквадратической ошибки MSE предсказания для трех способов устранения межкадровой избыточности видеоданных, используемых в методах Cinepak (кадровая разность), MPEG-2, MPEG-4 (блочная компенсация движения) и разработанном методе объектного предсказания изменения видеоданных (объектная компенсация движения). Из таблицы видно, что метод объектного предсказания изменения видеоданных обеспечивает уменьшение ошибки предсказания примерно в 6 раз по сравнению с методом Cinepak и примерно в 4,4 раза по сравнению с методами MPEG-2, MPEG-4.

Среднеквадратическая ошибка предсказания

Величина горизонтального смещения камеры	Среднеквадратическая ошибка MSE предсказания		
	Кадровая разность (Cinepak)	Блочная компенсация движения (MPEG-2, MPEG-4)	Объектное предсказание изменений видеоданных
1 см	2362	1294	215,364
2 см	3604	1868	615,367
3 см	3713	2202	623,401
4 см	3801	2802	624,219

Заключение

Предложен метод объектного предсказания изменения видеоданных при перемещении камеры на основе модели ее движения. Суть метода состоит в объектной декомпозиции опорного кадра видеоданных, классификации объектов по дальности, расслоении опорного кадра по дальности и формировании нового кадра на основе модели движения камеры, учитывающей смещения объектов навстречу вектору движения камеры. Метод обеспечивает уменьшение ошибки предсказания изменения видеоданных при движении камеры в 6 раз по сравнению с методом Cinepak и примерно в 4,4 раза по сравнению с методами MPEG-2, MPEG-4.

OBJECT PREDICTION CHANGES FOR VIDEO DATA TRANSFORMATION WITH HORIZENTAL CAMERA MOVMENT

T.M. AL-JUBOORI , V.YU. TSVIATKOU, V.K. KONOPELKO

Abstract

This is a suggested method for predicting the changes in the object in video data by using a model of camera motion. The method contains with, object decomposition of the reference frame of video data, the classification of objects in range, the start position of the reference frame for the range and the formation a new frame-based on the model of camera motion, taking in consideration, the displacement vector of the motion of objects towards the camera. The method provides a reduction of prediction error for video data changes when camera moves, through the use of information regarding characteristics of camera, installation conditions and parameters of camera motion.

Литература

1. *Iain R.* H // The Robert Gordon University. Aberdeen. UK. John Wiley & Sons Ltd. The Atrium. Southern Gate. Chichester. 2003. P. 306.
2. *A.B. Benitez, S. Chang* // Signals, Systems and Computers. Conference Record of the Thirty-Seventh Asilomar Conference. 2003. Vol.1 P. 92–96.
3. *Zhigang Z., Allen R.* // Eighth International Conference on Computer Vision (ICCV'01) 2001. Vol. 2. P. 723.
4. *Ianir I., Leonid P., Barak F.* // Real-time Image Processing Jornal. 2007. Vol. 2. P. 3–9.

УДК 621.391(075.8)

НОРМЕННОЕ ДЕКОДИРОВАНИЕ ОШИБОК ПОСРЕДСТВОМ ИХ МОДИФИКАЦИИ

В.А. ЛИПНИЦКИЙ, АЛЬ-ХАЙДАР Е.К.

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, Минск 220013, Беларусь

Поступила в редакцию 7 октября 2009

Предложен модифицированный норменный метод коррекции ошибок в двоичных БЧХ-кодах произвольной длины и произвольным кодовым расстоянием. Суть метода в отображении ошибок с не равной нулю первой компонентой синдрома в ошибки того же веса, но с нулевой первой компонентой синдрома.

Ключевые слова: линейный помехоустойчивый код, двоичный код, БЧХ-код, синдром ошибок, теория норм синдромов, норменный метод коррекции ошибок.

Введение

Жизнь в условиях современной информационной эпохи предъявляет жёсткие и противоречивые требования к передаче, обработке и хранению информации. Подавляющая часть телекоммуникационных систем (ТКС) функционирует с применением помехоустойчивых кодов. Теория и практика помехоустойчивого кодирования существует немногим более полувека, но переживает период постоянного и бурного развития, что отражается, в частности, в росте количества монографий и учебников, посвящённых данной теме (см., к примеру, [1 - 3]).

Теория норм синдромов [4, 5] предоставляет эффективный перестановочный норменный метод коррекции ошибок линейными кодами из семейства БЧХ-кодов. Этот метод обходится без решения уравнений в полях Галуа, на порядок уменьшает влияние проблемы селектора, даёт конструктивный подход к решению проблемы избыточности применяемых кодов, допускает техническую реализацию декодеров на однородных структурах.

Увеличение длин кодов и веса корректируемых ошибок замедляет работу и норменных методов коррекции ошибок, на новом витке актуализируя проблему селектора. В настоящее время идёт проработка различных подходов к дальнейшему сокращению объёма селектируемой совокупности ошибок. Оригинален метод выхода к ошибкам большей кратности [6]. В данной работе предлагается прямой подход, позволяющий сократить объём селектируемой совокупности $\Gamma-$орбит. Суть его в преобразовании искомого вектора-ошибки в класс векторов-ошибок с узко очерченным спектром значений норм, а именно, в класс векторов-ошибок того же веса, но с первой компонентой синдрома $s_1 = 0.$

Суть норменного метода

Норменный метод применяется к циклическим кодам – инвариантным относительно группы $\Gamma = \{\sigma, \sigma^2, ..., \sigma^n = id\}$ циклических сдвигов координат векторов, где $n-$ длина кода и для любого вектора $\bar{e} = (e_1, e_2, ..., e_n)$ $\sigma(\bar{e}) = (e_n, e_1, e_2, ..., e_{n-1}).$ Метод базируется на разбиении векторов-ошибок декодируемой совокупности K на $\Gamma-$орбиты – непересекающиеся между собой классы векторов-ошибок, переходящих друг в друга под

действием автоморфизмов группы Γ. $\Gamma-$орбиты содержат, как правило, по n различных векторов-ошибок, синдромы которых имеют чётко очерченный спектр.

Ряд циклических кодов позволяют находить нормы синдромов – инварианты $\Gamma-$орбит, вычисляемые через синдромы векторов-ошибок, не меняющиеся под действием σ на эти векторы, попарно различные для всех орбит декодируемой совокупности. При названных обстоятельствах суть норменного метода становится очевидной. При получении телекоммуникационной системой (ТКС) очередного вектора-сообщения $\bar{x}$ с ненулевым синдромом ошибок $S(\bar{x})$ вычисляется его норма синдромов $\overline{N} = \overline{N}(S(\bar{x}))$. Норма $\overline{N}$ однозначно указывает какой конкретно $\Gamma-$орбите J декодируемой совокупности K принадлежит вектор-ошибка $\bar{e}$ в сообщении $\bar{x}$. Зная какой-нибудь из векторов $\bar{e}_J$ $\Gamma-$орбиты J, сравнением синдромов $S(\bar{x})$ и $S(\bar{e}_J)$ несложно однозначно определить и сам вектор $\bar{e}$.

Таким образом, норменный метод систематизирует поиск в цепочке синдром – ошибка, да и существенно сокращает этот поиск, поскольку мощность множества ΓK $\Gamma-$орбит декодируемой совокупности K в n раз меньше мощности множества K.

Модифицированный норменный метод коррекции ошибок

Следует заметить, что с ростом n, а также с увеличением кратности корректируемых ошибок существенно увеличивается мощность $|\Gamma K|$, что сказывается на сложности декодера и скорости его работы. О сказанном свидетельствует следующая табл.1.

Таблица 1. **Количество ошибок и Г-орбит ошибок весом 2 – 4 на различных длинах**

Размерность n		7	15	31	63	127	255
Ошибки весом 2. Количество	ошибок	21	105	465	1953	8001	32385
	Г-орбит	3	7	15	31	63	127
Ошибки весом 3. Количество	ошибок	35	455	4495	39711	333375	2731135
	Г-орбит	5	31	145	631	2625	10711
	В т.ч. неполных	-	1	-	1	-	1
Ошибки весом 4. Количество	ошибок	35	1365	14465	595665	10334625	182061175
	Г-орбит	5	91	1015	9455	81375	674751

Следующая табл. 2 демонстрирует, что удельный вес векторов-ошибок с нулевой первой компонентой синдрома относительно невелик.

Таблица 2. **Количество T_ω векторов ошибок с $s_1 = 0$ весом $\omega = 3,4,5$ в двоичных БЧХ-кодах длиной $n = 7 \div 255$ а так же количество ΓT_3 – Г-орбит этих векторов**

T_ω и ΓT_ω	Длина БЧХ-кода n					
	7	15	31	63	127	255
T_3	7	35	155	651	2667	10795
ΓT_3	1	3	5	11	21	43
T_4	7	105	1085	39060	82677	680085
ΓT_4	1	7	35	620	651	2667
T_5	0	168	5208	103509	330708	33732216
ΓT_5	0	12	168	1643	2604	132284

Ниже рассматривается модификация норменного метода коррекции ошибок. В её основе лежит преобразование декодируемых ошибок, синдромы которых имеют ненулевую первую компоненту, в векторы ошибок с $s_1 \neq 0$.

Продемонстрируем модификацию норменного метода на наиболее обширном и важном для приложений классе БЧХ-кодов C_t с проверочной матрицей $H = (\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i})^T$, исправляющих $t-$кратные ошибки [1 – 3]. Здесь длина n кода C_t нечётна, делит число $2^m - 1$ для некоторого наименьшего натурального $m > 1$, а $\beta -$элемент порядка n мультипликативной группы поля Галуа $GF(2^m)$.

Пусть ТКС с кодом C_t приняла вектор-сообщение $\bar{x} = \bar{c} + \bar{e}$ с неизвестным вектором-ошибкой $\bar{e}$, но с известным синдромом $S(\bar{x}) = H \cdot \bar{x}^T = (s_1, s_2, ..., s_t)$ и предположительно, с весом t. Здесь $\bar{c} -$истинное сообщение. Пусть $x_1, x_2, ..., x_t -$локаторы ошибочных позиций принятого сообщения $\bar{x}$. Это элементы первой строки матрицы H как матрицы с элементами из поля $GF(2^m)$, соответствующие ошибочным позициям. Покоординатная запись векторного равенства $S = H \cdot \bar{x}^T$ приводит к следующей системе уравнений:

$$\begin{gathered} x_1 + x_2 + ... + x_t = s_1, \\ x_1^3 + x_2^3 + ... + x_t^3 = s_2, \\ \text{..... ....} \\ x_1^{2t-1} + x_2^{2t-1} + ... + x_t^{2t-1} = s_t. \end{gathered} \tag{1}$$

Предполагается, что $s_1 \neq 0$. От вектора-ошибки $\bar{e}$ перейдём к вектору $\bar{e}^*$ с локаторами ошибочных позиций

$$x_1^* = x_1 + s_1, \; x_2^* = x_2 + s_1, ..., \; x_t^* = x_n + s_1. \tag{2}$$

Система (1) для локаторов ненулевых координат вектора $\bar{e}^*$ преобразуется следующим образом.

$$x_1^* + x_2^* + ... + x_t^* = (x_1 + s_1.) + (x_2 + s_1) + ... + (x_t + s_1) = (t+1)s_1 = 0;$$

С учётом формулы $(a+b)^{2\tau+1} = (a^{2\tau} + b^{2\tau})(a+b) = a^{2\tau+1} + a^{2\tau}b + ab^{2\tau} + b^{2\tau+1}$ имеем

$$x_1^{*3} + x_2^{*3} + ... + x_t^{*3} = (x_1 + s_1.)^3 + (x_2 + s_1)^3 + ... + (x_t + s_1)^3 =$$

$$= (x_1^3 + x_2^3 + ... + x_t^3) + s_1(x_1 + x_2 + ... + x_t)^2 + s_1^2(x_1 + x_2 + ... + x_t) + ts_1^3 = s_2 + (t+2)s_1^3 = s_2 + s_1^3.$$

Аналогичные вычисления показывают, что

$x_1^{*5} + x_2^{*5} + ... + x_t^{*5} = (x_1 + s_1.)^5 + (x_2 + s_1)^5 + ... + (x_t + s_1)^5 = s_3 + s_1^5$; и так далее

$$x_1^{*(2t-1)} + x_2^{*(2t-1)} + ... + x_t^{*(2t-1)} = (x_1 + s_1.)^{2t-1} + (x_2 + s_1)^{2t-1} + ... + (x_t + s_1)^{2t-1} = s_t + s_1^{2t-1}.$$

Таким образом, из (1) получим следующую систему уравнений:

$$\begin{gathered} x_1^* + x_2^* + ... + x_t^* = 0, \\ x_1^{*3} + x_2^{*3} + ... + x_t^{*3} = s_2 + s_1^3, \\ \text{..... ....} \\ x_1^{*(2t-1)} + x_2^{*(2t-1)} + ... + x_t^{*(2t-1)} = s_t + s_1^{2t-1}. \end{gathered} \tag{3}$$

Как видим, в равенствах (3) первая компонента синдрома $S(\bar{e}^*) = (s_1^*, s_2^*, ..., s_t^*)$ равна нулю. Тогда у нормы синдрома $\overline{N} = \overline{N}(S(\bar{e}^*))$ первые $t-1$ координат принимают вырожденные значения ∞ или –. Совокупность ΓK имеет относительно немного $\Gamma -$орбит с такими координатами. Об этом свидетельствуют и данные табл. 2. Следовательно, процедура определения вектора ошибок $\bar{e}^*$, а с ним и вектора $\bar{e}$, легко реализуется норменным методом.

Пример 1. Пусть ТКС функционирует на основе БЧХ-кода C_7 длиной 31 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ для примитивного элемента α поля $GF(2^5)$, корня полинома $x^5 + x^4 + x^2 + x + 1$. Пусть приёмное устройство ТКС приняло сообщение с синдромом ошибок $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$. В этом случае система (1) имеет вид:

$$\begin{cases} x_1 + x_2 + x_3 = \alpha^{28}, \\ x_1^3 + x_2^3 + x_3^3 = \alpha^{29}, \\ x_1^5 + x_2^5 + x_3^5 = \alpha^{28}. \end{cases} \quad (4)$$

Сделаем в (4) замену $x_1 = x_1^* + \alpha^{28}$, $x_2 = x_2^* + \alpha^{28}, ..., x_t = x_t^* + \alpha^{28}$. Получим

$$\begin{cases} x_1^* + x_2^* + x_3^* = 0, \\ x_1^{*3} + x_2^{*3} + x_3^{*3} = \alpha^{24}, \\ x_1^{*5} + x_2^{*5} + x_3^{*5} = \alpha^{29}. \end{cases}$$

Как известно [1, 2], в коде C_7 норма синдрома $\bar{N} = (N_1, N_2, N_3)$, где $N_1 = s_2 / s_1^3$; $N_2 = s_3 / s_1^5$; $N_3 = s_3^3 / s_2^5$. Тогда $\bar{N}^* = \bar{N}(S(\bar{e}^*)) = (\infty, \infty, \alpha^{29})$. Табл. 2 указывает на наличие в данном БЧХ-коде C_7 лишь пяти Г-орбит тройных векторов-ошибок с $s_1 = 0$. В табл. 3 приведен весь список этих Г-орбит.

Таблица 3. **Образующие Г-орбит тройных ошибок, их синдромы и нормы синдромов в (31, 16) – БЧХ-коде C_7 с нормой вида $\bar{N} = (\infty, \infty, \beta)$**

№ п/п	Образующая $\bar{e}_i$	Синдром $S(\bar{e}_i)$	Норма $\bar{N}_i = \bar{N}(S(\bar{e}))_i$
1	$(1, 2, 20)$	$(0, \alpha^{20}, \alpha^{12})$	$(\infty, \infty, \alpha^{29})$
2	$(1, 3, 8)$	$(0, \alpha^{9}, \alpha^{24})$	$(\infty, \infty, \alpha^{27})$
3	$(1, 5, 15)$	$(0, \alpha^{18}, \alpha^{17})$	$(\infty, \infty, \alpha^{23})$
4	$(1, 4, 12)$	$(0, \alpha^{14}, \alpha^{18})$	$(\infty, \infty, \alpha^{15})$
5	$(1, 10, 16)$	$(0, \alpha^{24}, \alpha^{19})$	$(\infty, \infty, \alpha^{30})$

Из табл. 3 следует, что вектор $\bar{e}^*$ принадлежит Г-орбите J, порождённой вектором $\bar{e}_{орб} = (1, 2, 20)$ – с ненулевыми координатами на первой, второй и 20-й позициях. Осталось определить величину циклического сдвига вектора $\bar{e}_{орб} = (1, 2, 20)$ для получения $\bar{e}^*$. Конкретное значение этой величины получается сравнением синдромов $S(\bar{e}_{орб}) = (0, \alpha^{20}, \alpha^{12})$ и $S(\bar{e}^*) = (0, \alpha^{24}, \alpha^{29})$. Если в БЧХ-коде C_7 синдром $S(\bar{e}) = (s_1, s_2, ..., s_t)$, то синдром $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2, ..., \alpha^{2t-1} \cdot s_t)$ [4 –5].

Существует такое натуральное k, что $\sigma^k(\bar{e}_{орб}) = \bar{e}^*$. Следовательно, $20 + 3k = 24 + 31l$ для подходящего целого l или $3k = 4 + 31l$. Подберём наименьшее l, при котором $31l + 4$ делится на 3. Легко видеть, что требуемое $l = 2$. Тогда $31l + 4 = 66 = 3 \cdot 22$, то есть $k = 22$. Следовательно, $\bar{e}^* = (11, 23, 24)$. Поэтому $x_1^* = \alpha^{10}$, $x_2^* = \alpha^{22}$, $x_3^* = \alpha^{23}$. Тогда

$x_1 = x_1^* + \alpha^{28} = \alpha^{10} + \alpha^{28} = \alpha^9$, $x_2 = x_2^* + \alpha^{28} = \alpha^{22} + \alpha^{28} = \alpha^{13}$, $x_3 = x_3^* + \alpha^{28} = \alpha^{23} + \alpha^{28} = \alpha^{21}$.

Вычисленные локаторы однозначно высвечивают искомую вектор-ошибку $\bar{e} = (10, 14, 22)$.

Замечание. *Отметим, что рассмотренное преобразование локаторов (2) допустимо только при выполнении одного трудно проверяемого условия: ни один из локаторов* x_i *ненулевых координат искомого вектора-ошибки* $\bar{e}$ *не должен совпадать с* s_1. *Дело в том, что тогда* $x_i^* = 0,$ *а таких локаторов проверочная матрица БЧХ-кода* C_t, *очевидно, не имеет. Для тройных ошибок названное требование выполняется: если бы, скажем,* $s_1 = x_1 + x_2 + x_3 = x_1,$ *то тогда* $x_2 + x_3 = 0,$ *то есть* $x_3 = x_2,$ *что невозможно – локаторы координат векторов попарно различны.*

Заключение

Разработана модификация норменного метода коррекции ошибок. Реализуется путём отображения этих ошибок в ошибки того же веса, но с первой компонентой синдрома, равной нулю. Спектр таких ошибок небольшой по сравнению с их общим количество. Это существенно ускоряет работу декодера. Особенно эффективен метод при коррекции кодами трёхкратных ошибок.

NORM DECODING OF ERRORS VIA THEIR MODIFICATIONS

V.A. LIPNITSKI, E.K. AL-HAIDAR

Abstract

Modified norm decoding method of errors in binary BCH random length and random distance codes had been proposed. The essence of this method is in mapping errors with the first nonzero syndrome component in the error with the same weight where the first syndrome component is equal to zero.

Литература

1. *Мак-Вильямс, Ф.Дж.* // Теория кодов, исправляющих ошибки. М., 1979.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
3. *Конопелько, В.К., Липницкий, В.Д. Дворников и др*. Теория прикладного кодирования: Учебное пособие. М., 2004.
4. *Конопелько, В.К., Липницкий В.А*. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М., 2000.
5. *Липницкий В.А*. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. М., 2007
6. *Курилович А.В., Липницкий В.А., Аль-Хайдар Е.К. //* Докл. БГУИР. 2005, №6. 28 – 30.

УДК 621.391.14

МЕТОД И ХАРАКТЕРИСТИКИ ВЛОЖЕННОГО КОДИРОВАНИЯ ГРУППОВЫХ КОДОВ НА ОСНОВЕ ЦИКЛИЧЕСКОЙ ПОДСТАНОВКИ КОРРА

АЛЬ-АЛЕМ АХМЕД САИД, А.И. КОРОЛЕВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск 20013, Беларусь

Поступила в редакцию 13 октября 2009

Выполнена оценка эффективности предложенного метода вложенного кодирования групповых кодов, построенных на основе циклической подстановки Корра. Определены основные параметры циклического кода и канального кодека, реализующего метод вложенного кодирования и приведен сравнительный анализ рассчитанных параметров с параметрами известных кодов. Показано, что для практических целей достаточно использовать циклическую подстановку Корра степени $\alpha = 3$. В качестве внутреннего кода используется базовый (исходный) групповой (циклический) код с реализацией в декодере алгоритма декодирования базового группового кода.

Ключевые слова: групповой код, циклический код, кодер, декодер, кодек, кодовая последовательность, модуль ошибок, пакет ошибок, порождающая матрица, проверочная матрица, скорость кода, перемежение.

Общие принципы построения модифицированных групповых кодов на основе циклической подстановки Корра

Высокую скорость декодирования кодовых последовательности (КП) двоичных групповых кодов при минимальной сложности реализации декодирующих устройств (декодеров) обеспечивают алгебраические алгоритмы декодирования, а именно, мажоритарный, пороговый и синдромный. Однако данные алгоритмы декодирования чаще всего используются для коррекции случайных (независимых) ошибок. Кроме того, количество кодов, обеспечивающих реализацию данных алгоритмов существенно ограничен. Увеличить количество кодов и их корректирующую способность представляется возможным на основе использования циклической подстановки Корра и метода вложенного кодирования сформированных групповых кодов.

В соответствии с [1-3] сущность циклической подстановки Корра состоит в организации “внутреннего” перемежения (разнесения) информационных (кодовых) символов на основе которых осуществляется формирование проверочных уравнений (проверок на четность) базового двоичного группового кода.

Утверждение 1. Модифицированный групповой ($\alpha \cdot n$; $\alpha \cdot k$; $\alpha \cdot d_o$) – код построенный на основе базового (исходного) циклического (n ; k ; d_o) – кода путем циклической подстановки Корра степени $\alpha \geq 2$ корректирует любые $\alpha \cdot t$ или менее ошибочных символов при формировании $\alpha \cdot м$ проверочных уравнений ; $t \leq \frac{d_o\text{-}1(2)}{2}$ и $t \leq \frac{\mu}{2}$ ошибочных символов, корректируемых соответственно при синдромном и мажоритарном алгоритмах декодирования.

Данное утверждение легко доказывается построением конкретного модифицированного группового кода. Пусть в качестве исходного группового кода используется циклический максимальной длины с параметрами:

$$(n;k;d_0)=(7;3;4),\ R=k/n=3/7=0,428,\ P(x)=x^4+x^3+x^2+1,\ h(x)=x^3+x^2+1,$$

$$t_{\text{исп.}}\le\frac{d_0-1}{2}=3-1/2=1 \text{ бит и } \text{r}=(1\text{-R})\cdot100\%=(1\text{-}0{,}428)\cdot100\%=57{,}2\%$$

Для декодирования кодовых последовательностей (КП) используется мажоритарный алгоритм с формированием проверочных уравнений (проверок) а на основе проверочной матрицы вида (б):

а)

$$\begin{aligned}
&м_1=a_1=a_1',\\
&м_2=a_1\oplus a_2\oplus a_4,\\
&м_3=a_2\oplus a_3\oplus a_5,\\
&м_4=a_3\oplus a_4\oplus a_6,\\
&м_5=a_4\oplus a_5\oplus a_7,
\end{aligned}$$

где $\oplus$ - знак суммирования двоичных символов по модулю два.

б)

$$\text{H}_{(7,4)}\begin{bmatrix}1101000\\0110100\\0011010\\0001101\end{bmatrix}, \qquad (1)$$

Примем значение циклической подстановка $\alpha=2$. В результате чего модифицированный циклический код (ЦК) будет иметь следующие параметры:

$$(\alpha\cdot n;\alpha\cdot k;\alpha\cdot d_0)=(2\cdot7;2\cdot3;2\cdot4)=(14;6;8),\ P_{\text{м}}(x)=x^{\alpha\cdot4}+x^{\alpha\cdot3}+x^{\alpha\cdot2}+1=x^8+x^6+x^4+1,$$

$$h_{\text{м}}(x)=x^{\alpha\cdot3}+x^{\alpha\cdot2}+1=x^6+x^4+1,\ t_{\text{исп.м}}\le\frac{\alpha\cdot d_0-1(2)}{2}=\frac{2\cdot4-2}{2}=\frac{8-2}{2}=3 \text{ ошибочных}$$

двоичных символа, $R_m=k/n=6/14=0,428,\ \ r=(1-R_m)\cdot100\%=(1-0,428)\cdot100\%=57,2\%$

Проверочная матрица модифицированного ЦК будет иметь следующее построение:

$$\text{H}_{(14,6)}\begin{bmatrix}10100010000000\\01010001000000\\00101000100000\\00010100010000\\00001010001000\\00000101000100\\00000010100010\\00000001010001\end{bmatrix}. \qquad (2)$$

Из структуры данной проверочной матрицы следует, что для реализации мажоритарного алгоритма декодирования необходимо формировать $M=(k+2)$ проверочных уравнений с порогом принятия решения $П\ge\frac{M}{2}$; (с учетом тривиального соотношения $a_1 = a_1^{/}$ будет сформировано $M'=M+1$ проверочных уравнении). В этом случае все ошибочные информационные символы кратностью $t_{\text{ош.}}\le3$ будут скорректированы.

Например: пусть передавалась по каналу связи КП вида: $F(x)=00000000000000$, а на вход мажоритарного декодера поступила КП вида $F'(x)=11100000000000$ (старшие информационные символы слева), т.е. принятая КП содержит пакет ошибок из трех информационных символов. В декодере в соответствии проверочной матрицей (2) для данной структуры ошибок будут сформированы проверочные уравнения результатами. $A_1 \div A_3$ для первого, второго и третьего информационного символа соответственно (рис.1.).

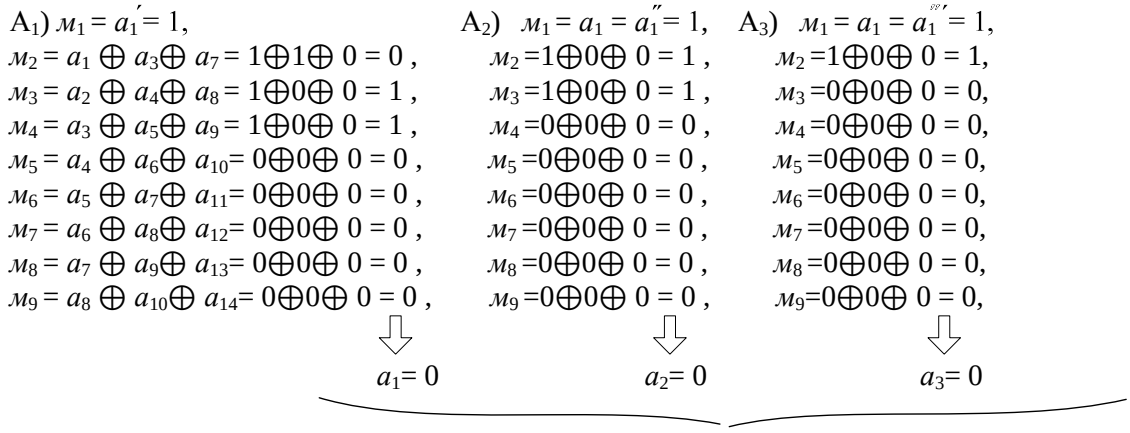


Рис.1. Сформированы проверочные уравнения результатами. $A_1 \div A_3$ для первого, второго и третьего информационного символа в декодере

Таким образом, все ошибочные информационные символы скорректированы. Аналогичным образом можно показать, что модифицированный $(\alpha \cdot n; \alpha \cdot k; \alpha \cdot d_0) = (14; 6; 8)$ – код обеспечивает коррекцию трех информационных символов $(t_{\text{исп.}} \le \frac{8-2}{2} = 3)$ при реализации синдромного алгоритма декодирования.

Метод вложенного кодирования групповых кодов на основе циклической подстановки

Возможность построения модифицированных групповых кодов на основе циклической подстановки Корра позволяет реализовать эффективный метод вложенного кодирования данных кодов, используя в качестве внутреннего базовый ЦК(при двух ступенях кодирования; базовый ЦК и модифицированный(ые) групповой(ые) код(ы)) – при трех и более ступенях кодирования. В соответствии с [4,5] для практического применения вложенного кодирования групповых кодов достаточно использование 2-3 ступеней кодирования.

На рис. 2 и рис. 3 приведены обобщенные структурные схемы соответственно кодера и декодера, реализующие двухступенчатое вложенное кодирование-декодирование информации на основе базового ЦК с параметрами (7;3;4) (внутренний код) и модифицированного ЦК (внешний код).

В декодерах данных кодов используется синдромный алгоритм декодирования, обеспечивающий высокое быстродействие декодирования кодовых последовательностей.

В соответствии с рис.2. информационные ($a_7 \div a_9$) и проверочные ($\alpha_1 \div \alpha_4$) символы второго канала кодирования (базового ЦК Хэмминга) суммируются по модулю два с проверочными ($в_1 \div в_7$) символами первого канала кодирования (модифицированного кода). В результате чего формируются семь потоков символов псевдослучайной последовательности:

$$\Pi_1 = в_1 \oplus a_7, \Pi_2 = в_2 \oplus a_8, \Pi_3 = в_3 \oplus a_9, \Pi_4 = в_4 \oplus \alpha_1, ..., \Pi_7 = в_7 \oplus \alpha_4;$$

проверочный символ $в_8$ первого канала кодирования передается без преобразования.

В декодере (рис.3) осуществляется одновременно формирование проверочных ($в_1' \div в_8'$) символов первого канала декодирования (модифицированного кода) и кодовых ($a_7' \div a_9'$, $\alpha_1' \div \alpha_4'$) символов второго канала кодирования (базового ЦК Хэмминга). Далее осуществляется поэтапно декодирование КП ЦК Хэмминга, формировании проверочных ($\alpha_1 \div \alpha_4$) символов второго канала декодирования, восстановление проверочных ($в_1 \div в_7$) символов перворго канала

декодирования и декодирование КП модифицированного кода. Для согласования по задержке декодированных информационных символов первого и второго каналов используется буферное устройство БУ.

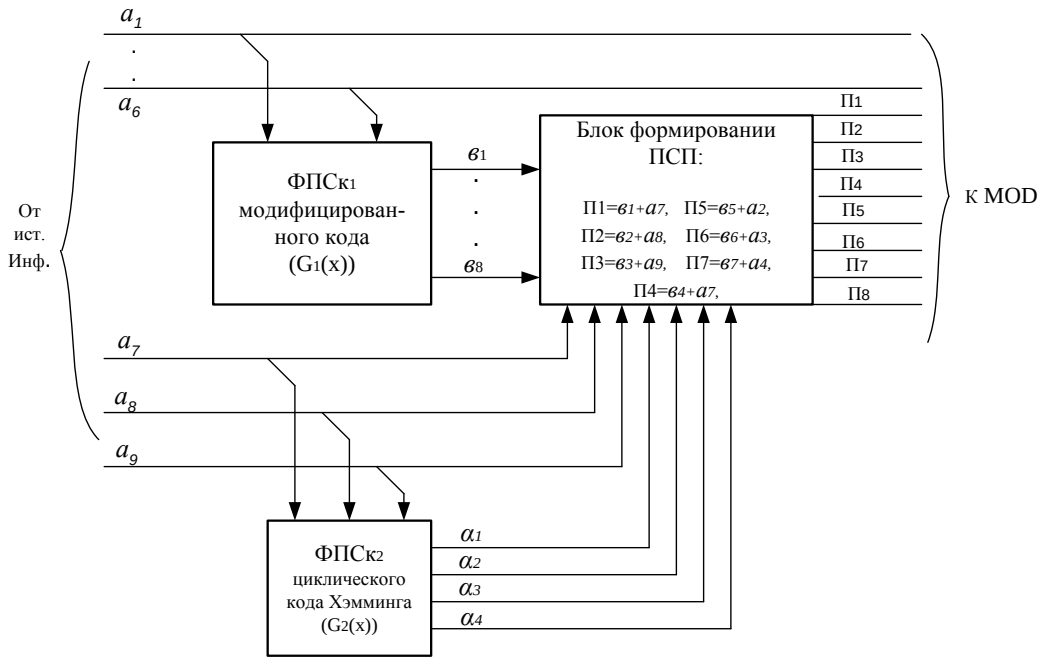


Рис. 2. Кодирующие устройство модифицированного ЦК: ФПСк$_1$ и ФПСк$_2$ – формирователи проверочных символов соответственно первого и второго каналов кодирования; ПСП – псевдослучайная последовательность

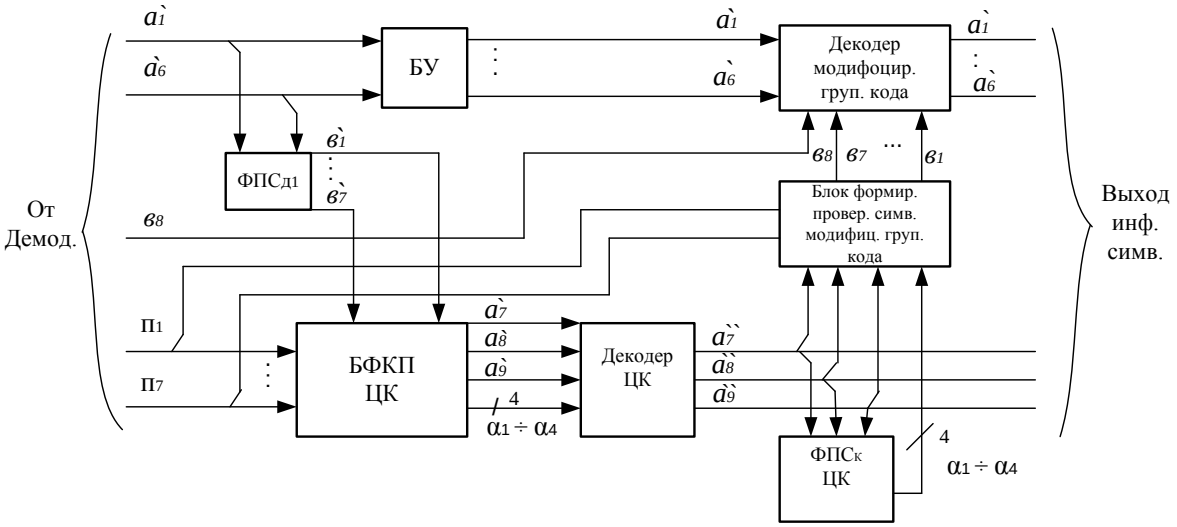


Рис. 3. Декодирующие устройство модифицированного ЦК: БУ – буферное устройство, БФКП – блок формирования кодовых последовательностей, ФПСд$_1$ – формирователь проверочных символов декодера модифицированного группового кода

В соответствии с рис.1. информационные ($a_7 \div a_9$) и проверочные ($\alpha_1 \div \alpha_4$) символы второго канала кодирования (базового ЦК Хэмминга) суммируются по модулю два с проверочными ($в_1 \div в_7$) символами первого канала кодирования (модифицированного кода). В результате чего формируются семь потоков символов псевдослучайной последовательности:

Оценка эффективности метода вложенного кодирования групповых кодов

Для оценки эффективности метода вложенного кодирования групповых кодов необходимо получить выражения количественно и качественно определяющие параметры данного метода, а именно: $R_B = k_B / n_B$ – скорость передачи кода; $d_{ов}$ – минимальное кодовое расстояние; $t_{исп.\ в}$ – общую кратность исправляемых ошибочных информационных символов; алгоритмы декодирования, обеспечивающие минимальную задержку информации и сложность реализации кодека, измеряемую количеством ячеек памяти.

Оценку параметров метода вложенного кодирования групповых кодов выполним для двух ступеней (каналов) кодирования-декодирования групповых кодов: полученные выражения не трудно обобщить на $N(N>2)$ ступеней кодирования.

Утверждение 2. Если $R_1 = k_1 / n_1$ – скорость передачи кода первой ступени (первого канала) кодирования и $R_2 = k_2 / n_2$ – скорость передачи кода второй ступени (второго канала) кодирования, то скорость передачи кода $R_в$, на основе которого реализуется метод вложенного кодирования групповых кодов, больше наибольшей скорости передачи используемых кодов, т.е. $R_B \geq R_{i\max}$, где $i \in 1;2.$

Доказательство. Избыточность используемых групповых кодов первого и второго каналов кодирования соответственно равны: $r_1 = \frac{n_1 - k_1}{n_1} = \frac{l_1}{n_1}$ и $r_2 = \frac{n_2 - k_2}{n_2} = \frac{l_2}{n_2}$.

Так как в соответствии с методом вложенного кодирования производится суммирование по модулю два символов КП второго канала и проверочных символов первого канала кодирования, то избыточность КП группового кода, реализующего метод вложенного кодирования будет равна произведению избыточностей исходных групповых кодов т.е. $r_в = r_1 \cdot r_2$.

Так как $r_1 < 1$ и $r_2 < 1$, то их произведение будет меньше наименьшего из сомножителей т.е. $r_в < r_{i\,min}$, где $i \in 1;2$.

Следовательно, скорость передачи группового кода $R_в = 1 - r_в$, на основе которого реализуется метод вложенного кодирования групповых кодов, будет больше наибольшей скорости передачи исходного группового кода, т.е.

$$R_B = 1 - r_B \rangle r_{i\max},\ i \in 1;2, \qquad \text{ч.т.д.} \tag{3}$$

Утверждение 3. Если d_{01} и d_{02} – соответственно минимальные кодовые расстояния исходных групповых кодов и $d_{01} \neq d_{02}$, то минимальное кодовое расстояние $d_{0в}$ группового кода, на основе которого реализуется метода вложенного кодирования информации , будет не менее максимального кодового расстояния исходного кода, т.е. $d_{0в} = \max.\ d_{01}, d_{02}$.

Доказательство данного утверждение обеспечивается использованием в кодеке двух каналов кодирования – декодирования и двух групповых кодов с разной корректирующей способностью: $d_{01} \langle\rangle d_{02}$. Следовательно, ошибки минимальной кратности корректируются обоими кодами, а ошибки максимальной кратности корректируются только один из кодов с наибольшим значением минимального кодового расстояния(в приведенной структурной схеме кодека модифицированный ЦК Хэмминга используемой в первом канале кодирования имеет наибольшее минимальное кодовое расстояние, а именно, $d_{01} = 8$). Исходя из того следует, что минимальное кодовое расстояние $d_{ов}$ группового кода, на основе которого реализуется метод вложенного кодирования – декодирования исходных групповых кодов, будет не менее максимального минимального кодового расстояния из исходных групповых кодов, т.е.

$$d_{0в} = \max.\ d_{01}, d_{02}\ , \qquad \text{ч.т.д.} \tag{4}$$

При $d_{01} = d_{02}$, $d_{ов} = d_{oi}$, $i \in 1;2$.

Утверждение 4. Максимальная кратность ошибок $t_{корр.в}$ корректируемые кодеком реализующего метод вложенного кодирования – декодирования исходных групповых кодов, удовлетворяет следующему равенству – неравенству:

$$t_{корр.в} \leq t_{корр.1} + t_{корр.2}\ , \tag{5}$$

где $t_{\text{корр.1}}$ и $t_{\text{корр.2}}$ – кратность ошибок корректируемых групповыми кодами первого и второго канала кодирования соответственно.

Доказательство данного утверждения выполним численным расчетом для кодека, реализующего вложенное кодирование групповых кодов с параметрами:

$(n_1; k_1; d_{01}) = (14; 6; 8)$ и $(n_2; k_2; d_{02}) = (7; 3; 4)$.

Наличие двух каналов декодирования и организация процедуры коррекции ошибок первоначально во втором канале кодека обеспечивает разделение ошибок по КП групповых кодов, а далее осуществляется поэтапное (последовательное) исправление ошибок данными кодами. Таким образом, независимые ошибки кратностью $t_{\text{корр.2}} \le \frac{d_{02} - 1(2)}{2}$ двоичных символов будет исправлены базовым ЦК Хэмминга, а группирующиеся ошибки кратностью $t_{\text{корр.1}} \le \frac{d_{01} - 1(2)}{2}$ двоичных символов будет исправлены модифицированным групповым кодом. Следовательно, общее количество корректируемых ошибок кодеком.

$$t_{\text{корр.В}} \le t_{\text{корр.1}} + t_{\text{корр.2}}, \qquad \text{ч.т.д.}$$

Задержка информации при декодировании метода вложенного кодирования зависит от используемых алгоритмов декодирования групповых кодов и способа передачи информации.

В соответствии со структурной схемой кодека (рис.1 и рис.2) минимальная задержка информации при декодировании будет обеспечиваться при реализации синдромного алгоритма декодирования и практически будет зависит от выбранного способа передачи информации.

При параллельном способе передачи информации задержка информации при декодировании будет определяться способом реализации кодека и выбранной элементной базой.

При последовательном способе передачи информации и синдромном алгоритме декодирования начальная задержка информации декодера равна длине КП модифицированного кода; для рассматриваемых групповых кодов начальная задержка информации $L_{\text{задер.синдр.}} = 14$ тактам.

При реализации мажоритарного алгоритма декодирования и последовательного способа передачи информации задержка информации будет составлять: $L_{\text{задер.синдр.}} \approx: L_{\text{задер.2k}} + L_{\text{задер.1k}} \approx (n_2 + k_2) + 2(n_1 + k_1)$ тактов, где $L_{\text{задер.2k}}$ и $L_{\text{з а д е р}}$ – задержка информации при декодировании во втором и в первом каналах соответственно.

Заключение

В данной статье предложен метод вложенного кодирования и декодирования групповых кодов, когда в качестве внешнего кода используется групповой код, построенный на основе известного циклического кода путём подстановки Корра. Определены основные характеристики группового кода при использовании двух каналов кодирования и декодирования, которые могут быть легко обобщены на групповые коды с большим количеством каналов кодирования – декодирования. Установлено, что метод вложенного кодирования и декодирования групповых кодов обеспечивает формирование кодов с характеристиками отличными от известных: при равной скорости кодов (равной избыточности кодов) модифицированный групповой код и метод вложенного кодирования – декодирования обеспечивает коррекцию ошибок большей кратности.

Для практического применения предложенного метода кодирования информации достаточно реализация двухканального кодека на основе базового и модифицированного групповых кодов. Минимальная задержка информации при декодировании обеспечивается при использовании синдромного алгоритма декодирования и параллельного способа передачи информации.

В данной статье не рассматривались вопросы организации цикловой синхронизации и сложности реализации кодека, которые требуют самостоятельных исследований.

Метод вложенного кодирования – декодирования групповых кодов может быть обобщен на сверточные коды.

METHOD AND CHARACTERISTIC CODING GROUP OF EMBEDDED CODES BASED ON CYCLIC SUBSTITUTION CORR

ALALEM AHMED SAID, A.E. KOROLEV

Abstract

Completed assessment of the effectiveness of the proposed method the embedded coding group codes constructed on the basis of a cyclic substitution Corr. The main parameters of a cyclic code and the channel codec that implements the method of the embedded coding and comparative analysis of calculated parameters with the parameters of known codes. It is shown that for practical purposes it is sufficient to use the cyclic substitution Corr degree $\alpha = 3$. As an internal code used by the base (initial) group (cyclic) code with the implementation of the decoder algorithm for decoding the base of the group code.

Литература

1. *Блейхут, Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
2. *Кларк, Дж*. Кодирование с исправлением ошибок в системах цифровой связи. М., 1986.
3. *Морелос – Сарагоса, Р*. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение. М., 2005.
4. *Колесник В.Д.* Декодирование циклических кодов. М., 1968.
5. *Конопелько В.К., Аль-алем Ахмед Саид, А.И. Королев.* Устройство вложенного кодирования и декодирования групповых кодов // Заявка №. А 20080773. М., 2008.

УДК 621.391

FADING COUNTERMEASURE FOR HIGH FREQUENCY DATA COMMUNICATONS USING ERRORS CORRECTING CODES

PHAM KHAC HOAN [1], DANG XUAN HAI [2], VU SON HA[3]

[1,2] *Le Quy Don Technical University, Ha noi, Viet Nam*
[3] *Institute of Information Technology, Ha noi, Viet Nam*

Submitted 13 October 2009

High Frequency (HF) data communication links remain relevant even in today's satellite era because they offer beyond line-of-sight without third-party equipment's and expensive satellite services. The disadvantage is that HF is a difficult medium to use, with significant channel distortion and background noise at any given frequency. This has severely limited the maximum data rate on HF data modems. In this paper the medium data rate communications on HF channels over seawater is considered using different approaches forward error correction (FEC) coding with adequate waveforms, and comparative evaluations are presented.

Keywords: high frequency, forward error correction coding, waveform, modem

Introduction

In the past, HF radio dominated beyond line-of-sight (BLOS) traffic. Data rate was limited by fading (due to multipath propagation), so that for a long time, the effective limit at long range was 75 symbols per second. Much higher rates are possible at shorter ranges, where is only one propagation path (surface wave). In recent years, data rates have risen impressively. Using a computer to sample transmissions and correct for distortions raises the data rate in a single tone to about 2400 bps.

The HF channel offers particularly intriguing challenges. The skywave channel provides support for long-haul beyond line of sight (BLOS) communications without the need for relays. However, the fading which is experienced on these circuits can be severe, and only a small percentage of skywave channels will support communications at data rates of up to 9600 bps. HF surface wave propagation provides BLOS communications as the wave propagates over the curved surface of the earth. How far beyond line of sight depends strongly on the composition of the surface. The HF surface wave propagates for distances of several hundred kilometers over highly conductive surfaces such as seawater, much farther than over fresh water or land. This phenomenon makes HF surface wave communications particularly significant for naval applications.

Signal fading and impulsive noise on HF channels significantly degrade the signal-to-noise ratio (SNR) of the received signal, leading to large burst of errors. Demodulators can reduce the number of errors by introducing error-control coding and data interleaving. The application of error control coding strategies to existing HF modems has resulted in significant performance improvements. In this paper we review the major problems encountered when waveform designing for communications over the HF band and an effective approach FEC coding for reliable naval HF data communications is investigated.

The factors affecting waveform design

The unique characteristics of the HF channel itself offer significant challenges. The ionospheric refraction which allows HF radio signals to propagate over long distances is not without its shortcomings. The received sky-wave signal may suffer distortion in the form of temporal dispersion (delay spread) as well as fluctuation in the signal’s amplitude and phase (Doppler spreading). It is reported that the amplitude of the received signal is Rayleigh distributed, while the

phase of the received signal is generally taken to be uniformly distributed. More typical mid-latitude sky-wave channels might show delay spreads of 1 - 4 ms with Doppler spreads of 1 Hz or less [1]. However, more typical values are 2 ms and 1 Hz respectively which are the basic parameters of standardized CCIR Poor channel. In the CCIR Good channel the two paths are separated by 0.5 ms and fade slowly at 0.1 Hz [2, 3]. In addition to the sky-wave channel, the HF surface wave channel offers interesting features and challenges. Over sea-water, the HF surface wave propagates far beyond line-of-sight, offering intriguing capabilities for Naval forces. As the surface wave begins to weaken at the periphery of the surface wave coverage region, a Rician channel is observed, with the non-fading component from the surface wave, and another, fading component, arising from a sky-wave path. The noise environment in the HF channel is also somewhat unique. CCIR Recommendation 322 provides a model for the HF noise environment. In general, it is much more impulsive than additive white Gaussian noise, with a much higher peak to mean ratio and tends to introduce burst error events.

One of biggest constraints for HF waveform design, particularly in recent years as the emphasis has shifted to higher data rates, is the channel bandwidth. Each HF communications channel bandwidth is typically limited to 3 kHz. The available bandwidth and the channel characteristics serve to limit the data rates which are achievable over HF. With the adoption of the modem serial-tone modem, naval broadcasts are moving to a 300 bps data rate and other services are being provided at rates up to 2400 bps. The demand for increased data rates imposed by modem networking protocols has led to a determined effort to push achievable data rates upward and has resulted in new and developing standards for waveforms offering rates of 9600 bps and greater. The context in which these systems are being developed is also changing. At one time, it is considered that paramount and most HF transmissions were one way, with no acknowledgment to give away information on the recipient's position. Using more bandwidth allows higher data rates. This can be achieved using adjacent sidebands, for example using the upper and lower sideband gives a total of 6 kHz of bandwidth.

Synchronization is the process at the receiver of identifying that a transmission is present and determining its timing with sufficient accuracy to permit demodulation. Again, HF offers some unique challenges in this area. The extreme fading experienced over HF circuits means that it is possible that a fade could encompass the entire duration of the preamble, making detection difficult or impossible, even in channels where the average signal level is sufficient to permit fairly high rate communications. Designers have tried to mitigate this in two ways. STANAG 4285, for example, specifies an 80 symbol preamble which is reinserted every 256 symbols. This ensures that when the signal level rises to levels which will support communications, it can be detected and synchronized to. The disadvantage with this approach is that the ratio of data to known symbols is decreased. The alternative to this is to use an initial long preamble to ensure synchronization, and then only include known symbols where they are directly required to assist in demodulation. Long preambles, with durations of up to 4.8 s have been used. This is the approach which was taken in Mil-Std 188-110 A where the length of the preamble has been tied to the interleaver used; when short or no interleaving is selected, a 0.6 s preamble is sent while when long interleaving is specified, a 4.8 s preamble is used.

The degree of synchronization required depends upon the algorithm used to demodulate the data. Early techniques required synchronization which was accurate to the symbol. More modem algorithms operate effectively with synchronization which is accurate to within several symbols. This distinction can be critical at HF, where multi-path fading can result in a continually changing synchronization point. The other use for the synchronization preamble is frequency offset removal. The known symbols in the preamble are used to estimate and remove any frequency offset in the received signal.

From a waveform design perspective, the trade-offs which must be considered are the delay and reduced data rate resulting from adding symbols dedicated to synchronization versus the probability of missing a signal which could have been successfully demodulated if an insufficient number of symbols is used for synchronization.

Adaptive equalization (serial-tone, OFDM) and guard-time protection (OFDM) are common techniques used to combat the effects of ISI at HF band. Equalization is required for serial tone modulations where the symbol duration is small relative to the expected time dispersion, which is often as severe as several milliseconds. Multi-carrier and M-FSK modulations, on the other hand, do not, as a rule, require equalization since their symbol spacing is sufficiently large as to mitigate the effect of multipath delay spread for most channels. Most modern HF modems use equalization which

requires estimation of the channel impulse response. As a consequence, the waveform designer must provide sufficient opportunity to make channel estimations and to maintain and update them as required.

Error Correction Coding for HF data communication system

In order to combat the effects of fading, an FEC scheme combined with an interleaver is typically used. For the best performance, the size of the interleaver is chosen to be inversely proportional to fading rate. Unfortunately, some HF channel conditions (CCIR Good channel) suffer from very slow rates which require interleavers spanning between 1 to 2 minutes. If an interleaver is not long enough, the fading process becomes correlated and the expected coding gains of FEC schemes can degrade significantly when compared to an independent Rayleigh fading channel. Since long interleaver cause large latencies at the receiver, a trade-off between latency and performance is unavoidable.

There are a number of criteria which must be considered in selecting an FEC code. Performance, complexity, compatibility and proprietary rights issues are all significant factors in the choice of a code. The relative performance of various coding schemes varies with code rate, modulation and the acceptable error thresholds.

a. Convolutional codes

Convolutional codes are soft decision, bit-error correcting codes which are usually decoded with a near maximum likelihood detection process known as Viterbi decoding. When combined with adequate interleaving, they provide good performance in the fading channels found at HF. Convolutional codes perform poorly in burst error environments, which makes it critical to achieve sufficient interleaving to break up fades.

The rate l/2, constraint length 7 convolutional code with generator polynomials: $g_1(x) = x^6 + x^4 + x^3 + x + 1$, $g_2(x) = x^6 + x^5 + x^4 + x^3 + 1$ is commonly used for HF serial tone data transmission. Both Mil-Std 188-110 A and STANAG 4285 Annex E call for this code. When rates greater than l/2 are required, they can be achieved by puncturing the code. Rates lower than l/2 are achieved by repeating the bits output by the encoder. The advantage of the repetition strategy is that it is much simpler than developing alternate codecs for each data rate.

b. Reed-Solomon codes

Reed-Solomon codes (RS codes) are a class of symbol error correcting codes which provide good burst (module) error performance, particularly when erasures are used. The code itself provides an indication of error when it is not possible to correctly decode the received data. For example, a module error with 4-bit length can be corrected and a double module error can be identified at the same time using the norm criteria for RS code (72, 60) [4]. This feature can be very valuable in packet data systems. Relative to other coding schemes, RS codes work best at high rates or when the acceptable BER thresholds are particularly stringent. The major disadvantage associated with RS codes is the difficulty in incorporating soft decision information into the decoding process in a form more sophisticated than simple erasures.

c. Concatenated codes

Concatenated codes attempt to use multiple encodings to overcome the shortcomings of some codes. Powerful concatenated codes have been formed by using convolutional inner codes with RS outer codes. The main disadvantage of concatenated codes is that they require two interleavers to be effective. This limits the amount of interleaving which can be applied to the inner code, with the result that for the error rates usually considered adequate at HF, i.e., in the 10^{-3} to 10^{-5} range, concatenated codes generally do not perform as well as convolutional codes by themselves. However, if a very stringent BER criterion is required, they will perform very well.

d. Trellis Coded Modulation (TCM)

This class of codes exploits the improved minimum distance properties which can be obtained by combining coding and modulation. One significant advantage of TCM is the ease with which soft decision decoding can be implemented, resulting in further coding gains. Moreover, TCM is the ease of designing a family of modems which can transmit data at traditional rates. Much of the work in TCM has focused on channels with AWGN, but this is not valid for HF channels. HF in particular represents a difficult environment for TCM because of the interaction which takes place between the

coding and the equalizer. Recently, several researchers investigate the possibility of designing trellis codes suitable for fading channels where the decoder have access to perfect channel state information [3].

e. Iterative codes

Turbo codes are the best known example of iterative codes and able to be very close to the Shannon capacity bound. There are three drawbacks associated with these codes. To obtain the impressive performance that they offer, substantial interleaving is required. The computational complexity associated with these codes is substantially greater than convolutional codes, although significant strides have recently been made in reducing the computational complexity. Most of these codes are protected by patents and, as such, are subject to proprietary rights which makes their adoption for use at HF very problematic.

f. Interleaving

Depending on the kind of code employed, the interleaver may interleave symbols or bits. In the case of Reed-Solomon codes, in order to preserve the burst error capabilities of the code, symbols are interleaved. With convolutional and other bit error correcting codes, it is the bits which are interleaved. Both block and convolutional interleavers are used for HF data communications. The block interleaver has the advantage that if the data packets are sized to fit within an interleaver block, no flush is required. The drawback to the block interleaver is that it is only possible to synchronize at interleaver block boundaries. With a convolutional interleaver, on the hand, synchronization is possible once every cycle through the interleaver and, for the same end-to-end delay, better performance is achieved. The major disadvantage to the convolutional interleaver is that it requires a flush to clear out the interleaver at the end of the transmission.

Design of coded-waveform for naval reliable HF medium-data-rate communication

a) The comparison single-tone and parallel tone modems

Much of the early research into HF communications was undertaken and MIL-STD-188-110A describes three modems suitable for data rates of 2400 bps. In chronological order the modems are the 16-tone, 39-tone and single-tone modems. The three modems comprise two fundamentally different modem formats; the first two represent parallel tone modems, while the most recent addition uses only a single signalling tone.

The parallel-tone modem is able to extend the length of the channel symbol such that time-delay spread of the signal becomes a small fraction of the total symbol length. The advantages of the parallel-tone format are its simplicity and spectral efficiency. The disadvantage is the poor power efficiency. The second MIL-STD parallel-tone modem is the 39-tone. While the 16-tone modem was uncoded, the 39-tone modem uses a shortened (14, 10) Reed-Solomon code and gives a significant performance advantage.

For second format the waveform comprises a single tone, so a time-delay spread in the order of a few milliseconds causes significant amounts of ISI. To overcome this, an equalizer estimates and compensates the channel distortions, thereby removing the ISI. The MIL-STD single-tone modem uses probe sequences to measure the channel distortion. The probe sequence must be long enough to cope with the maximum amount of time-delay spread and frequent enough to allow the equalizer to track changes to the channel impulse response. The probe sequence does not carry data, so it represents lost signalling power. The advantage of the probe sequence is that it allows the demodulator to use coherent detection.

The other comparison is based on the interference tolerance of the two formats. Co-channel interference from other HF users is a problem. Even low levels of co-channel interference can seriously degrade the bit error rate (BER) performance of modems. We, therefore, consider the interference tolerance of the three MIL-STD modems. The performance of the 16-tone modem is worst of all, because of its simple demodulator and absence of error-control coding. The 39-tone modem with FEC tests reveal that it is also sensitive to the position of the interferer. When the interferer is placed on the centre of a signalling tone, it is very vulnerable, and has little to commend it over the 16-tone modem. When the interfering tone is placed between the signalling tones, the modem is the most robust, providing reliable data communications at signal-to-interferer ratios above 5 dB. In recent research OFDM modems are proposed for high data rate communications, however it is

necessary to cope with several problems, for example, excessive guard-time, reduce peak to average power ratio, the tone frequency offset, symbol timing recovery, and so on [3].

The single-tone modem is not sensitive to the frequency of the interferer and performs very well when the signal-to-interferer ratio is above 12 dB. As the level of the interferer increases the BER performance of the modem degrades rapidly. More recent versions of the single-tone modem are available with excision processing that can remove narrowband interference. To summarise, the performance of the single-tone modem is no better than the parallel-tone modems in the presence of interference. While it is possible to add interference excision processing before the demodulator, this is equally applicable to the parallel or single-tone modems. In either case, the deficiencies of the waveform require powerful error-control coding to give them credible performance.

b) Naval Application of HF Data Communications

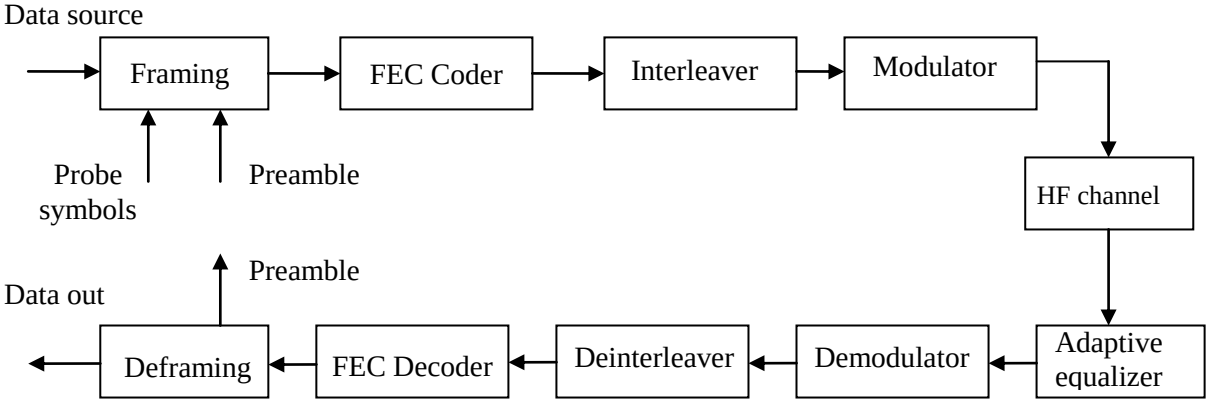
In general, the relative strengths of groundwave and skywave signals as a function of range behave. At short range, groundwave will dominate and at long range, skywave will be the primary propagation mechanism (Rayleigh channel). At intermediate ranges, there is a transition region where the Rician channel model is appropriate. An assessment was undertaken to obtain an indication of:

- the received signal levels and signal-to noise ratios (SNR) that could be expected by naval platforms at various ranges, and;
- the boundaries of the transition region between groundwave and skywave domination.

In Vietnam, island – to – shore and ship – to – shore communications typically are not long-haul path (the distance island – to – shore approximates 250 ÷ 370 nmi and nearer), therefore HF surface wave is able to use for these communicating situations. In this conditions a Rician channel is often observed, with the non-fading component from the surface wave, and another, fading component, arising from a sky-wave path. However, most naval broadcasts were run at 75 bps, and were often unreliable because of the lack of FEC coding.

Figure shows a structure scheme single tone modem data transfer at HF band with FEC coding and interleaving.

For medium data rate communications PSK is appreciate rather than FSK or QAM, in our scheme QPSK is chosen. In this scheme a binary Reed-Solomon is used for module errors correcting and identifying with using norm theory, which is investigated by professors B. K. Konopelko and V. A. Lipnitski [5]. In fact, with FEC scheme without ARQ and duplex transmission it is not necessary to detection uncorrected errors, but for hybrid scheme with duplex transmission it is unavoidable, therefore in our scheme the errors control strategy can be easily change. It is noted that in this scheme the symbol interleaver is used, that allows to increase to interleaving deep, thereby, the long burst errors are separated to shorter module errors. On the other hand, a module error can be corrected simpler and more effectively with the norm decoding. The smaller delay decoding compensates the interleaving delay. The other techniques (the probe symbols and adaptive equalizer) are similar to the existing.



Structure scheme single tone modem data transfer at HF band

Conclusions

A study of the current single and parallel-tone modem formats, revealed only minor advantages or disadvantages when considering the waveforms is presented. The parallel-tone modem was slightly more robust than the single-tone when considering tolerance to carrier wave interference. It is, however, necessary to cope with several problems, for example, excessive guard-time, reduce peak-to average power ratio, the tone frequency offset, symbol timing recovery, and so on. On the other hand, the complexity of the equalizers employed in the single-tone modem represents a considerable computational effort, and the probe symbols used to train the equalizer limit the maximum data rate that the modem can carry. In the proposed scheme, QPSK combinating with a Reed-Solomon coding, can be easily change errors control strategy, increase to interleaving deep and reduce decoding delay by using norm decoding.

References

1. *Jorgenson M.B., Moreland K.W. //* RTO IST Symposium on Tactical Mobile communications. 1999.
2. *Gill M.C. //* "The DORIC Program: HF modem technology", Technical report, Defence science and technology organization. 1995.
3. *Gill M.C. //* "Coded-Waveform Design for High Speed Data Transfer over High Frequency Radio Channels", PhD thesis, University of South Australia. 1998.
4. *Фам Хак Хоан* // Современные проблемы радиоэлектроники и телекоммуникации: 4 Меж. НТК, Севастополь, Украина, 2008.
5. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. М., 2007.

УДК 621.391

КОНТУРНОЕ ПОЗИЦИОНИРОВАНИЕ ПОЛУТОНОВЫХ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МОДИФИЦИРОВАННОГО ФИЛЬТРА РОБЕРТСА

О.ДЖ. АЛЬ-ФУРАЙДЖИ, В.Ю. ЦВЕТКОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 13 октября 2009

Предложен метод взаимного контурного позиционирования двух полутоновых изображений для обеспечения их сшивки. Суть метода состоит в формировании контурной маски на основе модифицированного фильтра Робертса для одного из позиционируемых изображений и ее использовании для поиска наилучшего варианта размещения одного изображения поверх другого, обеспечивающего максимальную похожесть областей перекрытия этих изображений. В качестве критерия максимальной похожести использован минимум среднеквадратической разности, вычисляемый для выделенных контурной маской пикселей на множестве возможных областей перекрытия изображений. Метод обеспечивает сокращение вычислительной сложности позиционирования полутоновых изображений за счет минимизации числа операций при формировании контурной маски на основе модифицированного фильтра Робертса и вычислении среднеквадратической разности областей перекрытия изображений в результате использования не всех, а только выделенных контурной маской пикселей в областях перекрытия.

Ключевые слова: позиционирование изображений, сшивка изображений, контурные маски, модифицированный фильтр Робертса.

Введение

В геоинформационных, телемедицинских, производственно-технологических и охранных системах широкое применение находят панорамные изображения. Для формирования панорамных изображений используются несколько разнесенных в пространстве камер с перекрывающимися областями видимости [1] или одна перемещающаяся панорамная камера [2]. В обоих случаях панорама формируется в результате сшивки изображений, имеющих области соответствия. Базовой операцией сшивки является взаимное позиционирование двух изображений, в результате которого определяется наилучший вариант размещения одного изображения поверх другого, обеспечивающий максимальную похожесть областей перекрытия этих изображений [3]. Позиционирование производится в сочетании с различными преобразованиями сшиваемых изображений (поворотами, масштабированием, цветовой и тоновой коррекцией, компенсацией аберраций оптической системы камеры и другими). По способу позиционирования методы сшивки изображений могут быть разделены на три основных класса. К первому классу относятся методы, в основе которых лежит поиск лучшего варианта совмещения двух изображений в результате последовательного перебора всех возможных вариантов для всех пикселей в областях перекрытия изображений [4]. Эти методы обеспечивают высокую точность позиционирования, но имеют высокую вычислительную сложность. Методы второго класса используют для сокращения вычислительной сложности позиционирования характерные ключевые пиксели сшиваемых изображений, выделяемые с помощью фильтров [5, 6]. Для методов второго класса характерны высокая вероятность ошибки позиционирования из-за неверного определения ключевых точек [6], резкое снижение эффективности с ростом точности позиционирования из-за увеличения вычислительной сложности процедуры фильтрации [5], ограничения на аппаратно-программную реализацию с использованием ПЛИС из-за высокой алгоритмической сложности, отсутствие возможности управления в широких пределах числом

ключевых пикселей и соответственно соотношением «вычислительная сложность – точность позиционирования» из-за ограничения диапазонов перестройки фильтров [5]. К третьему классу относятся комбинации методов первых двух классов [7], сочетающие их недостатки и труднореализуемые в реальном масштабе времени.

Цель данной работы – разработать вычислительно простой метод взаимного позиционирования двух полутоновых изображений, ориентированный на аппаратно-программную реализацию и обеспечивающий эффективное управление соотношением «вычислительная сложность – точность позиционирования».

Модель сшивки изображений

При сшивке изображение $I(n) = \left\| i(y,x) \right\|_{y=\overline{0,Y(n)-1},\, x=\overline{0,X(n)-1}}$ может быть представлено многопараметрической моделью, определяемой следующим выражением

$$I(n) = f_{PT}(P_S(n), P_C(n), P_O(n)), \tag{1}$$

где f_{PT} – функция проекционного преобразования, обеспечивающая получение двухмерной проекции трехмерной сцены; $n \in [0, N]$ – порядковый номер сшиваемого изображения; N – число изображений, используемых для сшивки; $P_S(n)$ – множество параметров трехмерной сцены; $P_C(n)$ – множество параметров оптоэлектронной системы видеокамеры; $P_O(n)$ – множество параметров пространственной ориентации видеокамеры.

В общем случае сшивка требует поиска на множестве $I(n)$ ($n = \overline{0, N-1}$) всех пар изображений $I(n_1)$ и $I(n_2)$ ($n_1 \in [0, N-1]$, $n_2 \in [0, N-1]$), которые имеют области соответствия и, следовательно, могут быть частично перекрыты, т.е. размещены одно поверх другого с некоторым смещением.

Описание метода взаимного позиционирования полутоновых изображений

Для обеспечения сшивки предлагается метод позиционирования двух полутоновых изображений $I(n_1)$ и $I(n_2)$ на основе контурных масок, позволяющий определять границы областей перекрытия $\tilde{I}(n_1, r) \subseteq I(n_1)$ и $\tilde{I}(n_2, r) \subseteq I(n_2)$ сшиваемых изображений в соответствии с выражением

$$\min(MSE_C(\tilde{I}(n_1, r), \tilde{I}(n_2, r))) \Rightarrow (\tilde{Y}, \tilde{X}) \tag{2}$$

при $r = \overline{0, R-1}$, где $MSE_C(\tilde{I}(n_1, r), \tilde{I}(n_2, r))$ – взвешенная среднеквадратическая ошибка, характеризующая различие областей перекрытия $\tilde{I}(n_1, r) = \left\| \tilde{i}^{(n_1, r)}(y,x) \right\|_{y=\overline{0,\tilde{Y}(r)-1},\, x=\overline{0,\tilde{X}(r)-1}}$ и $\tilde{I}(n_2, r) = \left\| \tilde{i}^{(n_2, r)}(y,x) \right\|_{y=\overline{0,\tilde{Y}(r)-1},\, x=\overline{0,\tilde{X}(r)-1}}$ сшиваемых изображений $I(n_1)$ и $I(n_2)$ для выделенных контурных точек; $\tilde{Y}(r)$, $\tilde{X}(r)$ – размеры по вертикали и горизонтали областей перекрытия $\tilde{I}(n_1, r)$ и $\tilde{I}(n_2, r)$; r – номер анализируемого варианта перекрытия; $R = (Y(n_1) + Y(n_2) - 1)(X(n_1) + X(n_2) - 1)$ – максимально возможное количество анализируемых вариантов перекрытия. Значение взвешенной среднеквадратической ошибки $MSE_C(\tilde{I}(n_1, r), \tilde{I}(n_2, r))$ определяется с помощью выражения

$$MSE_C(\tilde{I}(n_1, r), \tilde{I}(n_2, r)) = \frac{\sum_{y=0}^{\tilde{Y}(r)-1} \sum_{x=0}^{\tilde{X}(r)-1} \left(\tilde{i}^{(n_1, r)}(y,x) - \tilde{i}^{(n_2, r)}(y,x) \right)^2 \cdot m_C^{(n_1)}(y,x)}{\sum_{y=0}^{\tilde{Y}(r)-1} \sum_{x=0}^{\tilde{X}(r)-1} m^{(n_1)}(y,x)}, \tag{3}$$

где $m_C^{(n_1)}(y,x) = \theta(1)$ – коэффициент контурной маски $M_C(n_1) = \left\| m_C^{(n_1)}(y,x) \right\|_{y=\overline{0,Y(n_1)-1},\, x=\overline{0,X(n_1)-1}}$, вычисляемой для одного из изображений, например $I(n_1)$; $M_C(n_1) = f_C(I(n_1))$; f_C – функция выделения контуров изображения.

Предложенный метод взаимного позиционирования обеспечивает сокращение вычислительной сложности позиционирования двух полутоновых изображений $I(q_1)$ и $I(q_2)$ за счет минимизации числа операций при вычислении взвешенной среднеквадратической ошибки $MSE_C(\tilde{I}(q_1,r),\tilde{I}(q_2,r))$ для областей их перекрытия $\tilde{I}(q_1,r)$ и $\tilde{I}(q_2,r)$ в результате использования не всех, а только выделенных контурной маской $M_C(q_1)$ пикселей в областях перекрытия $\tilde{I}(q_1,r)$ и $\tilde{I}(q_2,r)$.

Метод состоит из следующих шагов.

1) Формирование контурной маски $M_C(q_1)$ для изображения $I(q_1)$.

2) Определение вертикальной B_Y и горизонтальной B_X границ зоны поиска областей перекрытия для изображения $I(q_2)$. Ограничение зоны поиска областей перекрытия необходимо для уменьшения вероятности ложного решения при вычислении выражения (2) на границах изображений $I(q_1)$ и $I(q_2)$, где число пикселей слишком мало. Количество $R' < R$ анализируемых вариантов перекрытия изображений определяется в соответствии с выражением

$$R' = Y' \cdot X', \tag{4}$$

где $Y' = Y(q_1) + Y(q_2) - 2 \cdot B_Y - 1$, $X' = X(q_1) + X(q_2) - 2 \cdot B_X - 1$ – число возможных ориентаций одного изображения поверх другого по вертикали и горизонтали.

3) Инициализация матрицы $M_{MSE_C} = \left\| m_{MSE_C}(y,x) \right\|_{y=\overline{0,Y'-1},\, x=\overline{0,X'-1}}$ взвешенной среднеквадратической ошибки в соответствии с выражением

$$m_{MSE_C}(y,x) = 0 \tag{5}$$

при $y = \overline{0,Y'-1}$, $x = \overline{0,X'-1}$.

4) Цикл вычисления взвешенной среднеквадратической ошибки $MSE_C(\tilde{I}(q_1,r),\tilde{I}(q_2,r))$ для всех возможных вариантов перекрытия изображений $I(q_1)$ и $I(q_2)$. Осуществляется вычисление элементов матрицы M_{MSE_C} взвешенной среднеквадратической ошибки в соответствии с выражением

$$m_{MSE_C}(y,x) = MSE_C(\tilde{I}(q_1,r),\tilde{I}(q_2,r)) \tag{6}$$

при $y = \overline{0,Y'-1}$, $x = \overline{0,X'-1}$, $r = y \cdot X' + x$.

5) Цикл поиска минимального элемента матрицы M_{MSE_C} взвешенной среднеквадратической ошибки. В результате перебора всех значений матрицы M_{MSE_C} определяются координаты $y_{\min}$ и $x_{\min}$ минимального элемента с помощью выражения

$$\min(M_{MSE_C}(y,x)) \Rightarrow y_{\min} = y, x_{\min} = y \tag{7}$$

при $y = \overline{0,Y'-1}$, $x = \overline{0,X'-1}$.

Координаты минимального элемента матрицы M_{MSE_C} определяют наилучший вариант перекрытия изображений $I(q_1)$ и $I(q_2)$, которому соответствуют области перекрытия $\tilde{I}(q_1,r)$ и $\tilde{I}(q_2,r)$ при $r = y \cdot X' + x$.

Для снижения вычислительной сложности метода на шаге 1 предлагается использовать стек для записи координат значимых (ненулевых) элементов контурной маски $M_C(q_1)$. В этом случае на шаге 4 для вычисления взвешенной среднеквадратической ошибки $MSE_C(\tilde{I}(q_1,r),\tilde{I}(q_2,r))$ используются только пиксели $\tilde{i}^{(q_1,r)}(y,x)$ и $\tilde{i}^{(q_2,r)}(y,x)$, координаты (y,x) которых совпадают с координатами значимых элементов контурной маски $M_C(q_1)$, записанными в стек. Необходимый размер стека определяется числом $N_S(q_1)$ значимых элементов контурной маски $M_C(q_1)$ с помощью выражения

$$N_S(q_1) = \sum_{y=0}^{Y(q_1)-1} \sum_{x=0}^{X(q_1)-1} m_C^{(q_1)}(y,x). \tag{8}$$

За счет использования стека координат значимых элементов контурной маски $M_C(1)$ при определении значений элементов матрицы M_{MSE_C} число операций $(i_{1,r}(y,x)-i_{2,r}(y,x))^2$ в выражении (3) сокращается до $R' \cdot N_S(1)$. При равенстве размеров сшиваемых изображений выигрыш χ от использования стека координат значимых элементов контурной маски для определения взвешенной среднеквадратической ошибки $MSE_C(I_{1,r}, I_{2,r})$ в сравнении с вариантом использования обычной среднеквадратической ошибки MSE определяется с помощью выражения

$$\chi = \frac{Y(1) \cdot X(1) + 2 \cdot \sum_{y=B_Y}^{Y(1)-2} \sum_{x=B_X}^{X(1)-2} (y+1) \cdot (x+1)}{R' \cdot N_S(1)}. \quad (9)$$

Выигрыш χ тем больше, чем меньше значимых элементов в контурной маске $M_C(1)$. Однако, сокращение числа $N_S(1)$ значимых элементов в контурной маске $M_C(1)$ и, как следствие, сокращение вычислительной сложности позиционирования ведет к увеличению вероятности и величины ошибки позиционирования. В этой связи актуальной задачей является разработка алгоритма выделения контуров объектов на изображении, позволяющего изменять число $N_S(1)$ значимых элементов в контурной маске $M_C(1)$ в широких пределах и эффективно управлять за счет этого соотношением «вычислительная сложность – точность позиционирования».

Алгоритм формирования контурной маски полутонового изображения

Предлагается алгоритм формирования контурной маски $M_C(1)$ полутонового изображения $I(1)$, основанный на статистической пороговой обработке результата вычитания от изображения $I(1)$ его сдвинутой копии (модифицированный фильтр Робертса) и позволяющий управлять числом $N_S(1)$ значимых элементов в контурной маске $M_C(1)$ в широких пределах для согласования его с заданным размером S_S стека за счет оценки вероятности появления пикселей в контурной маске с использования верхнего $T_H(1)$ и нижнего $T_L(1)$ порогов.

Алгоритм состоит из следующих шагов.

1) Цикл выделения контуров объектов изображения $I(1)$. Формируется контурное изображение $I_C(1) = \left\| i_C(y,x) \right\|_{y=\overline{0,Y(1)-1}, x=\overline{0,X(1)-1}}$, каждый пиксель которого определяется в соответствии с выражением

$$\begin{cases} i_C(y,x) = \left| i(y,x) - i(y-1,x-1) \right| \text{ при } y = 0, x = \overline{0, X(1)-1}, \\ i_C(y,x) = \left| i(y,x) - i(y-1,x-1) \right| \text{ при } y = \overline{0, Y(1)-1}, x = \overline{0, X(1)-1}. \end{cases} \quad (10)$$

2) Цикл вычисления вероятности появления пикселей в контурном изображении $I_C(1)$. Формируется одномерная статистическая матрица $M_S(1) = \left\| m_S(x) \right\|_{\left(x=\overline{0,2^{D_Y(1)}-1}\right)}$, каждый элемент которой после инициализации $m_S(x) = 0$ при $x = \overline{0,2^{D_Y(1)}-1}$ определяется с помощью выражения

$$m_S(i_C(y,x)) = m_S(i_C(y,x)) + 1, \quad (11)$$

при $y = \overline{0, Y(1)-1}$, $x = \overline{0, X(1)-1}$.

3) Цикл вычисления значения нижнего порога $T_L(1)$. После инициализации значений нижнего порога $T_L(1) = T_H(1)$ и суммы $N_S(1) = 0$ значимых элементов в контурной маске $M_C(1)$, осуществляется их переопределение исходя из значений элементов статистической

матрицы $M_S(\cdot)$ при заданных значениях верхнего порога $T_H(\cdot)$ и размера S_S стека, а также с помощью рекуррентного соотношения

$$(T_L(\cdot), N_S(\cdot)) = f_S(T_L(\cdot), N_S(\cdot), T_H(\cdot), M_S(\cdot)), \tag{12}$$

где f_S – функция статистической пороговой обработки, реализующая на каждой итерации операцию $(N_S(\cdot) \le S_S) \wedge (T_L(\cdot) > 0) \Rightarrow (T_L(\cdot) = T_L(\cdot) - 1) \wedge (N_S(\cdot) = N_S(\cdot) + m_S(T_L(\cdot)))$.

Полученное в результате значение нижнего порога $T_L(\cdot)$ позволяет согласовать число $N_S(\cdot)$ значимых элементов контурной маски $M_C(\cdot)$ с заданным размером S_S стека координат значимых элементов контурной маски и адаптироваться к заданному значению верхнего порога.

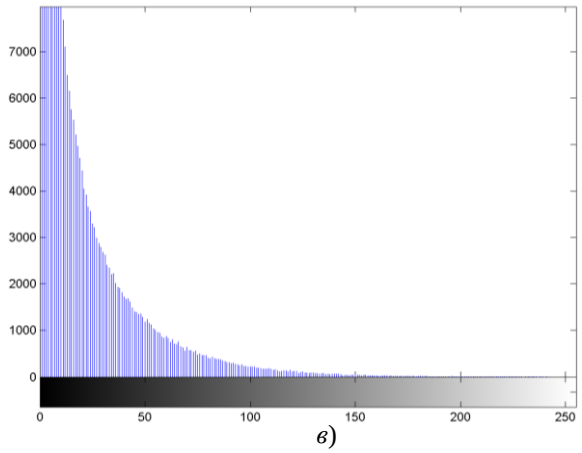
4) Цикл формирования контурной маски $M_C(\cdot)$. Элементы контурного изображения $I_C(\cdot)$ используются для вычисления элементов контурной маски $M_C(\cdot)$ с помощью выражения

$$m_C(y, x) = \begin{cases} 1 \ \textit{при} \ T_L < i_C(y, x) \le T_H, \\ 0 \ \textit{при} \ (i_C(y, x) \le T_L) \vee (T_H < i_C(y, x)) \end{cases} \tag{13}$$

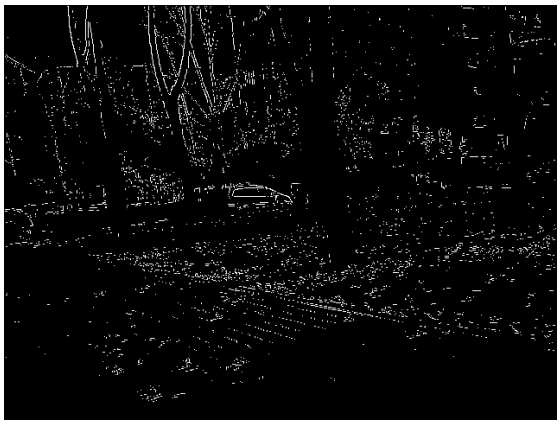
На рис. 1 приведены пример полутонового изображения $I(\cdot)$, результат $I_C(\cdot)$ его контурной обработки, визуальный образ одномерной матрицы $M_S(\cdot)$ (гистограмма контурного изображения $I_C(\cdot)$) и контурная маска $M_C(\cdot)$ (N= 12933 значимых пикселей) для $T_L(\cdot) = 80$ и $T_H(\cdot) = 160$.

а)

б)



в)



г)

Рис. 1. Формирование контурной маски при $T_L(\cdot) = 80$ и $T_H(\cdot) = 160$: *а* – полутоновое изображение $I(\cdot)$; *б* – контурное изображение $I_C(\cdot)$; *в* – гистограмма контурного изображения $I_C(\cdot)$; *г* – контурная маска $M_C(\cdot)$

Вычислительная сложность контурной обработки полутоновых изображений

Фильтр	Размер ядра фильтра	Число операций на пиксель (последовательная реализация)				Число операций (параллельно-конвейерная реализация)	Арифме-тика	
		Мультипли-кативных	Аддитив-ных	По модулю	Всего		Целочис-ленная	Дробная
Modified Roberts	2×2	0	2	1	3	2	x	
Sobel	3×3	4	13	2	19	3	x	
Roberts	2×2	0	5	2	7	2	x	
Prewitt	3×3	0	13	2	15	3	x	
LoG	9×9	81	81	1	163	3	x	x
Canny	$5\times5, 3\times3$	31	44	3	78	11	x	x

Оценка эффективности метода взаимного позиционирования изображений

Для оценки эффективности разработанного метода взаимного позиционирования полутоновых изображений использованы пары перекрывающихся изображений трехмерных сцен, полученные с помощью цифровой камеры при различном ее смещении. На рис. 2 представлено тестовое полутоновое изображение (рис. 2,*а*) и результат его взаимного позиционирования (рис. 2,*б*) с тестовым полутоновым изображением, представленным на рис. 1,*а*.

а) *б*)

Рис. 2. Взаимное позиционирование полутоновых изображений: *а* – полутоновое изображение; *б* – результат взаимного позиционирования

На рис. 3 представлены зависимости ошибки E_P позиционирования от числа N значимых пикселей контурной маски, полученной с помощью различных контурных фильтров. Ошибка позиционирования вычисляется с помощью выражения

$$E_P = \Delta y + \Delta x, \qquad (14)$$

где Δy, Δx – смещения по горизонтали и вертикали центра области перекрытия изображений, найденной с помощью метода позиционирования с использованием контурных масок на основе модифицированного фильтра Робертса, относительно центра области перекрытия изображений, найденной без использования контурных масок.

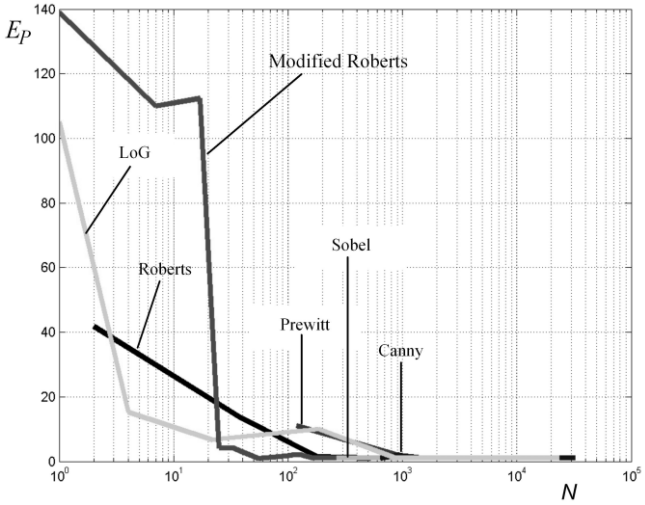


Рис. 3. Зависимости ошибки E_P позиционирования от числа N значимых пикселей контурной маски

Из рис. 3 видно, что использование модифицированного фильтра Робертса для формирования контурной маски эффективно при уменьшении числа значимых пикселей до значения 25. При этом для полутоновых изображений 480×640 пикселей с перекрытием 75% оценка ₡ выигрыша от использования стека координат значимых элементов контурной маски для определения взвешенной среднеквадратической ошибки составляет около 80 раз. Оценка ₡ выигрыша дает приблизительное значение выражения (9) и определяется по формуле

$$₡ = \frac{T_{MSE}}{T_{MSE_C}}, \qquad (15)$$

где T_{MSE} – время программного моделирования позиционирования полутоновых изображений с использованием всех пикселей области перекрытия для расчета значения среднеквадратической ошибки MSE; T_{MSE_C} – время программного моделирования контурного позиционирования полутоновых изображений с использованием значимых контурных точек области перекрытия для расчета значения взвешенной среднеквадратической ошибки MSE_C.

Заключение

Предложен метод взаимного контурного позиционирования двух полутоновых изображений для обеспечения их сшивки, основанный на модифицированном фильтре Робертса. Суть метода состоит в формировании контурной маски для одного из позиционируемых изображений и ее использовании для поиска наилучшего варианта размещения одного изображения поверх другого, обеспечивающего максимальную похожесть областей перекрытия этих изображений. В качестве критерия максимальной похожести использован минимум взвешенной среднеквадратической разности, вычисляемый для выделенных контурной маской пикселей на множестве возможных областей перекрытия изображений. Метод обеспечивает сокращение вычислительной сложности позиционирования полутоновых изображений в 2 и более раза за счет использования модифицированного фильтра Робертса для контурной обработки и до 80 раз за счет вычисления взвешенной среднеквадратической разности областей перекрытия изображений с использованием не всех, а только выделенных контурной маской пикселей в областях перекрытия.

CONTOUR POSITIONING BASED ON MODIFIED ROBERETS FILTER FOR GRAYSCALE IMAGES

O.J. AL-FURAIJI, V.YU. TSVIATKOU

Abstract

In this paper a method, of mutual contour positioning of two grayscale images to stitch them together, is proposed. The essence of the method includes forming a contour mask based on the modified Roberts filter for one of the positioned images and using it to find the best position option of one image over another, i.e., providing the maximum similarity between the overlap areas of these images. A minimum mean-square difference is used as a criterion for the maximum similarity, and is computed for the selected contour mask pixels in the set of possible overlapping areas of images. The method reduces the computational complexity of positioning the grayscale images by minimizing the number of operations because of forming the contour mask on the basis of the modified Roberts filter and calculating the mean square difference between the overlapping areas of images by using not all but only selected contour mask pixels in the areas of overlap.

Литература

1. *Zoghlami I., Faugeras O., Deriche R.* // IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’97).Puerto Rico. June 1997. P. 420–425.
2. *Szeliski R., Shum H-Y.* // SIGGRAPH '97, Proceedings of the 24th Annual Conference on Computer Graphics, Los Angeles, CA, USA, 3-8 August 1997. P. 251–258.
3. *Capel D., Zisserman A.* // IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR’98). USA. June 1998. P. 885–891.
4. *Szeliski R., Kang. S. B.* Direct methods for visual scene reconstruction // IEEE Workshop on Representation of Visual Scenes, Cambridge, MA, USA. June 1995. P. 26–33.
5. *Gonzalez R.C., Woods R.E.* // Digital image processing. Upper Saddle River, Prentice Hall. 2002. P. 793.
6. *Brown M., Lowe D. G.* // International Journal of Computer Vision. 2007. Vol. 74. P. 59–73.
7. *Shum H-Y., Szeliski R.* // International Journal of Computer Vision. February 2000. Vol. 36. № 2. P. 101–130.

УДК 621.391

МЕТОДЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИИ ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ В МЕЖСЕТЕВЫХ ЭКРАНАХ

М.Н. БОБОВ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 13 октября 2009

Технология трансляция сетевых адресов (Network Address Translation (NAT)) осуществляется на межсетевом экране, стоящем на границе между внутренней сетью, и внешней сетью. Перед посылкой пакетов во внешнюю сеть, NAT транслирует внутренние локальные адреса в глобальные уникальные IP-адреса и наоборот. Эта технология осуществляется для скрытия внутренних адресов своей сети, чтобы не дать злоумышленнику возможности получить информацию о структуре и масштабах сети, а также о структуре и интенсивности исходящего и входящего трафиков.

Ключевые слова: межсетевой экран (МСЭ), локальный и глобальные адреса, внутренние и внешне адреса, таблица NAT.

Введение

МСЭ осуществляющий трансляцию адресов, должен иметь, по меньшей мере, один внутренний и один внешний интерфейс [1]. В обычных условиях NAT конфигурируется на МСЭ, являющемся для данной локальной сети выходом в глобальную сеть. Когда пакет покидает внутреннюю сеть, NAT транслирует локальный адрес источника в глобальный уникальный адрес. Когда пакет входит в локальную сеть, NAT транслирует глобальный адрес назначения в локальный адрес. Если существует более одной выходной точки в глобальную сеть, то все устройства, работающие с NAT, должны иметь идентичные таблицы трансляции. Если программное обеспечение не может транслировать адрес, оно блокирует пакет и посылает сообщение источнику протоколом ICMP “хост не доступен” [2].

МСЭ, на котором NAT сконфигурирован, не должен передавать наружу информацию о внутренней сети. Тем не менее, данные о маршрутизации, получаемые извне (из внешней сети), могут передаваться в локальную сеть.

Трансляция внутреннего адреса источника

Используется для преобразования внутренних адресов в глобальные адреса при связи с внешними сетями. Включает в себя статическую или динамическую трансляцию:

- *Статическая трансляция* устанавливает взаимно-однозначное соответствие между внутренними локальными адресами и внутренними глобальными адресами. Статическая трансляция полезна, когда внутренний хост должен быть доступен извне по фиксированному адресу.

- *Динамическая трансляция* устанавливает соответствие между внутренними локальными адресами и пулом глобальных адресов.

На рис. 1 показан МСЭ, транслирующий адрес источника при переходе пакета из внутренней сети во внешнюю сеть.

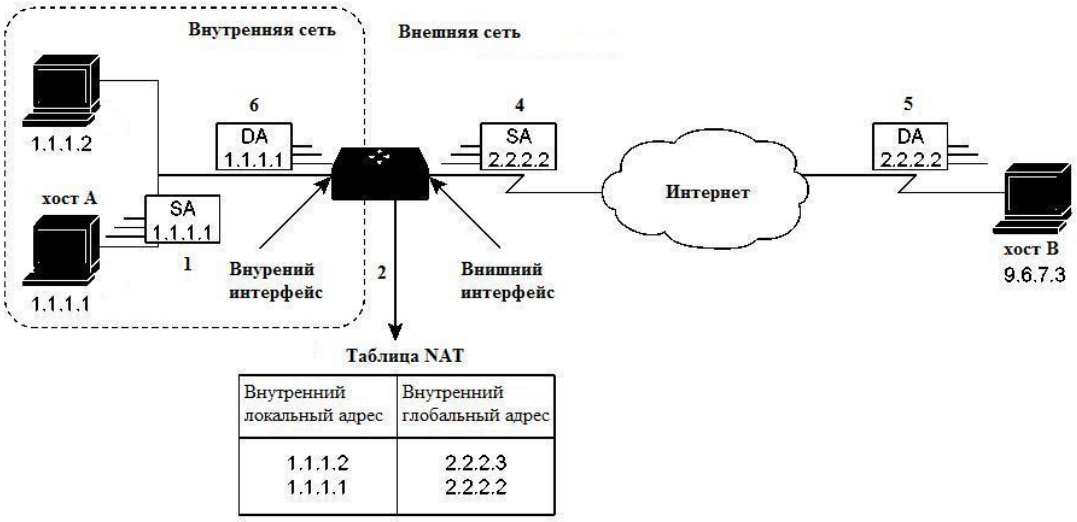


Рис. 1. Трансляция внутренних адресов: SA ≡ Адрес источника (Source Address);
DA ≡ Адрес назначения (Destination Address)

Статический метод трансляции.

В соответствии с рис. 1, трансляция внутренних адресов источника статическим методом включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает пакет от хоста 1.1.1.1, читает информацию из заголовка и сверяется со своей NAT-таблицей.
3. Если входа трансляции не существует в таблице, МСЭ блокирует пакет.
4. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
5. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).
6. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.
7. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятый.

Алгоритм этого механизма представлен на рис. 2.

Динамический метод трансляции.

Трансляция внутренних адресов источника динамическим методом включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется со своей NAT-таблицей.
3. Если вход трансляции не существует в таблице, МСЭ определяет, что адрес источника 1.1.1.1 должен транслироваться динамически, выбирает легальный глобальный адрес из пула динамических адресов и создает вход в таблице трансляции. Этот тип входа называется *простым входом*.
4. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
5. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).
6. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.
7. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

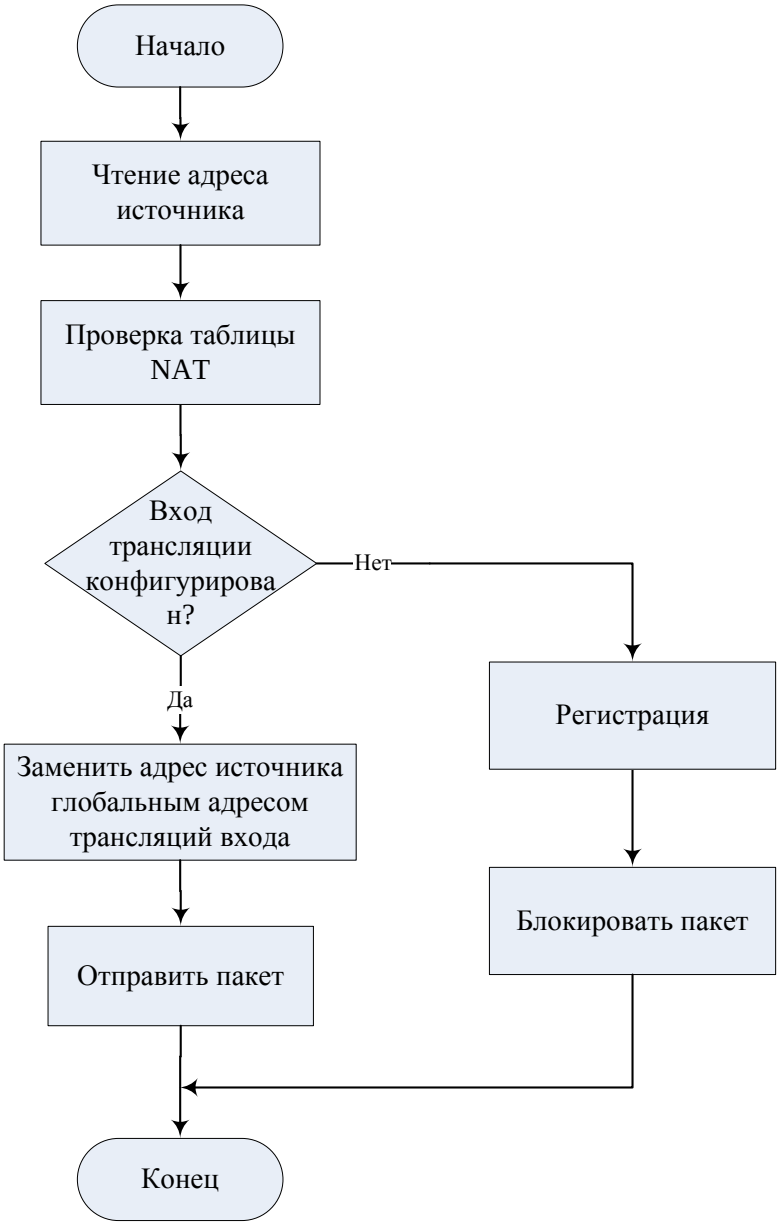


Рис. 2. Алгоритм трансляции внутреннего адреса источника статическим методом

Смешанный метод трансляции.

Трансляция внутренних адресов источника смешанным методом, включает следующие шаги:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется со своей NAT-таблицей.

a. Если статический вход трансляции был сконфигурирован, МСЭ следует на шаг 3.

b. Если вход трансляции не существует в таблице, МСЭ определяет, что адрес источника 1.1.1.1 должен транслироваться динамическим методом, выбирает легальный глобальный адрес из пула динамических адресов и создает вход в таблице трансляции. Этот тип входа называется *простым входом*.

3. МСЭ заменяет внутренний локальный адрес источника хоста 1.1.1.1 (SA=1.1.1.1) на глобальный адрес, в соответствии с входом в таблице, и отправляет пакет.
4. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес назначения 2.2.2.2 (DA=2.2.2.2).

5. Когда МСЭ получает пакет с внутренним глобальным адресом, он проверяет NAT-таблицу, транслирует адрес во внутренний локальный адрес хоста 1.1.1.1 и направляет пакет хосту 1.1.1.1.

6. Хост 1.1.1.1 получает пакет и продолжает диалог с хостом B. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

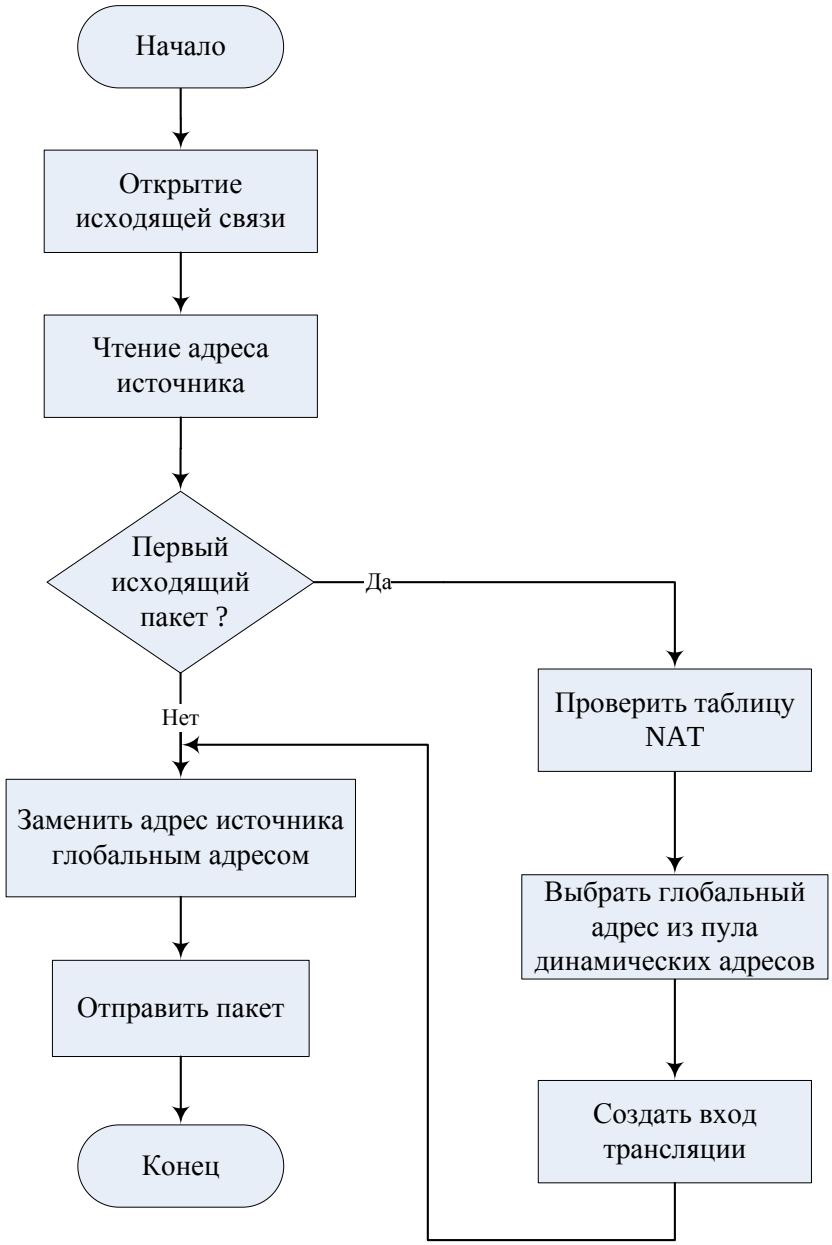


Рис. 3. Алгоритм трансляции внутреннего адреса источника динамическим методом

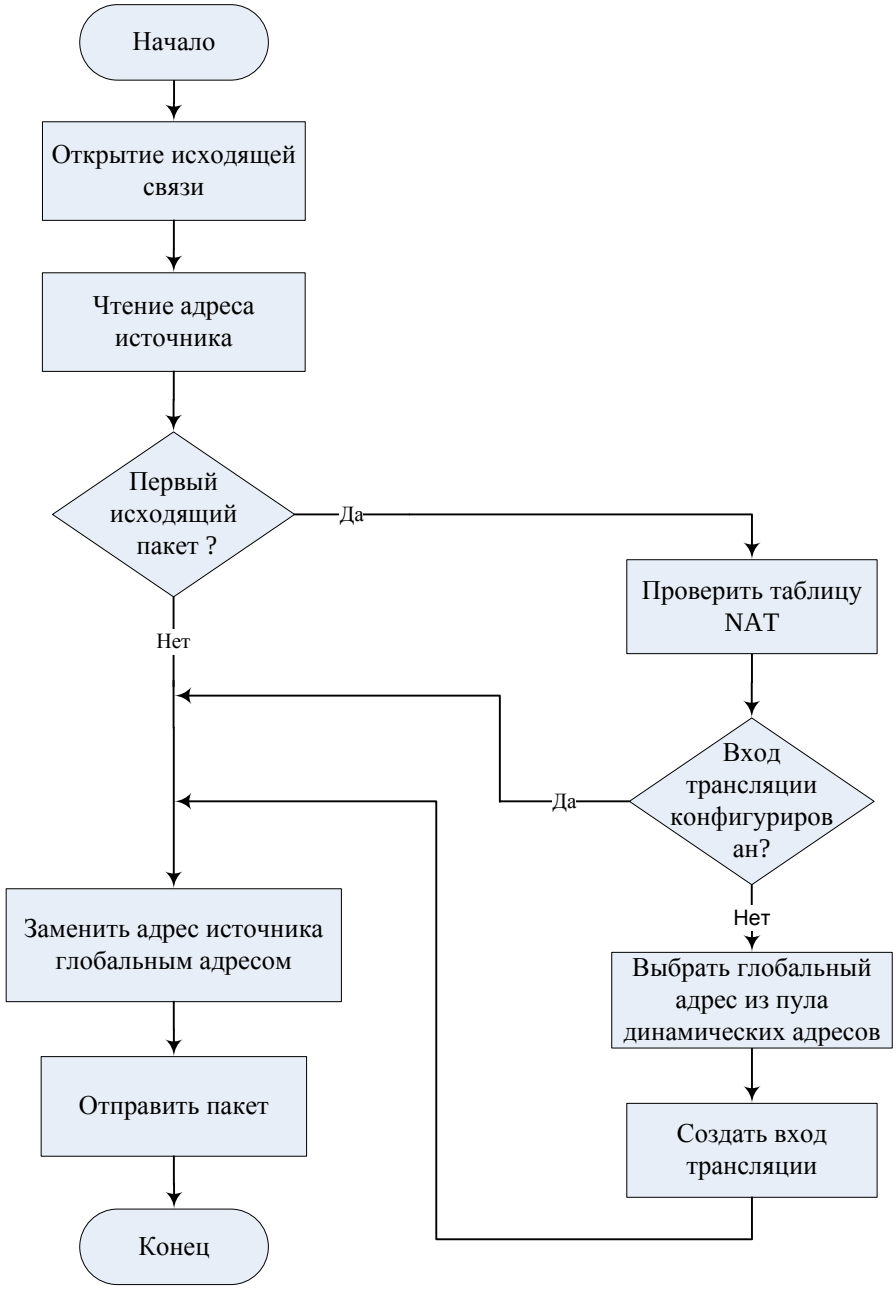


Рис. 4. Алгоритм трансляции внутреннего адреса источника смешанным методом

Совмещение внутренних глобальных адресов

Данный режим трансляции (режим совмещения) позволяет сэкономить адреса в пуле внутренних глобальных адресов путем настройки МСЭ на использование одного глобального адреса для нескольких локальных адресов. Когда такой режим сконфигурирован, МСЭ имеет достаточно информации от протоколов верхних уровней (например, номера портов TCP или UDP) для трансляции глобального адреса обратно в нужный локальный адрес. Когда нескольким локальным адресам ставится в соответствие один глобальный адрес, номера портов TCP или UDP каждого внутреннего хоста позволяют различать их локальные адреса [3].

Рис. 5 иллюстрирует механизм трансляции адресов, когда один внутренний глобальный адрес представляет несколько внутренних локальных адресов. Номер порта TCP играет роль отличительного признака.

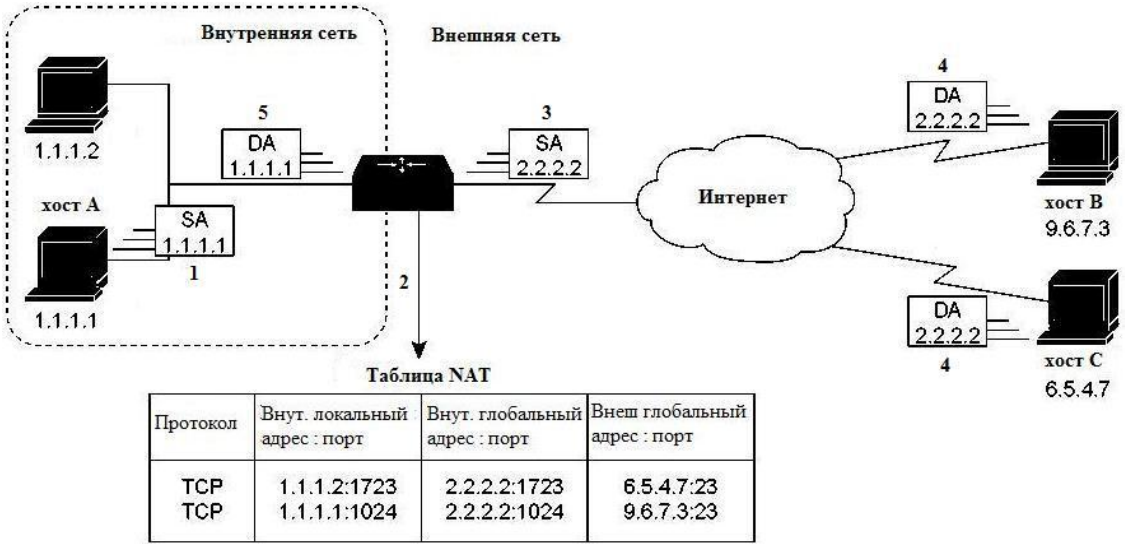


Таблица NAT

Протокол	Внут. локальный адрес : порт	Внут. глобальный адрес : порт	Внеш глобальный адрес : порт
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

Рис. 5. Перегрузка глобальных адресов в NAT

В данном режиме трансляции внутренних глобальных адресов, как показано на рис. 5, хост B и хост C представляют, что они взаимодействует с одном хостом по адресу 2.2.2.2. Реально, они сообщаются с разными хостами в виду отличия номеров портов. МСЭ реализует этот механизм следующими шагами [4, 5]:

1. Пользователь на хосте 1.1.1.1 открывает соединение с хостом B.
2. МСЭ получает первый пакет от хоста 1.1.1.1, читает заголовок и сверяется своей NAT-таблицей.

a. Если вход трансляции в таблице не существует, МСЭ транслирует внутренний локальный адрес 1.1.1.1 в легальный глобальный адрес. Если совмещение адресов разрешено и другая трансляция является активной, то МСЭ использует тот же глобальный адрес для создания входа и сохраняет информацию, необходимую для обратной трансляции. Этот тип входа называется *расширенным входом.*

3. МСЭ заменяет локальный адрес источника 1.1.1.1 на выбранный глобальный адрес и отправляет пакет.
4. Хост B получает пакет и отвечает хосту 1.1.1.1, используя глобальный адрес 2.2.2.2.
5. Когда МСЭ получает пакет с глобальным адресом, он проверяет NAT-таблицу, используя в качестве ключа тип протокола, внутренний глобальный адрес и номер порта, транслирует адрес во внутренний локальный адрес 1.1.1.1 и направляет пакет хосту 1.1.1.1.
6. Хост 1.1.1.1 получает пакет и продолжает сетевой обмен. Для каждого пакета МСЭ повторяет действия шагов со второго по пятой.

Алгоритм этого механизма представлен на рис. 6.

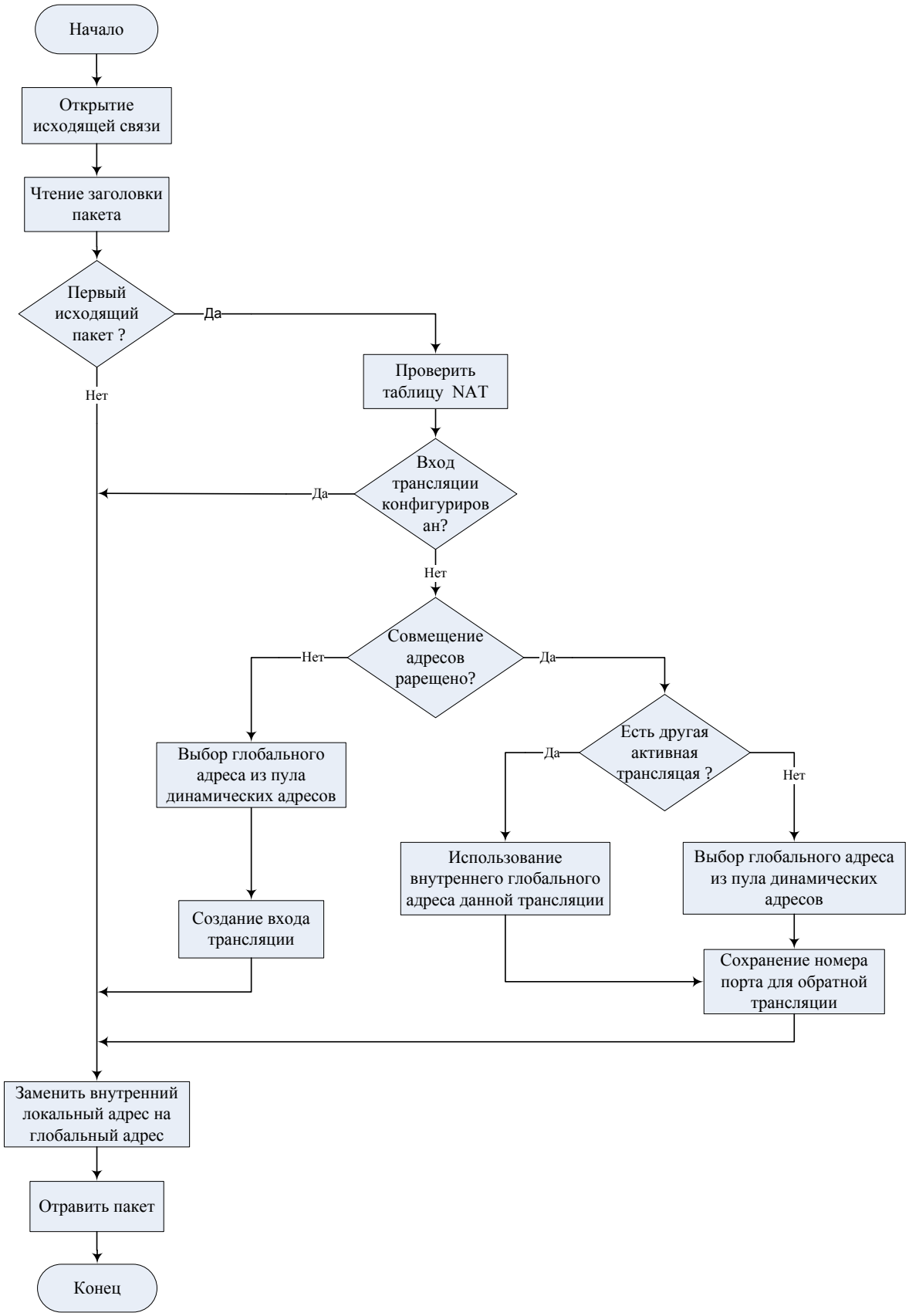


Рис. 6. Алгоритм совмещения внутренних глобальных адресов

Заключение

Технология трансляции сетевых адресов является одним из самых эффективных механизмов используемых для скрытия структуры и масштабов сети, а также структуры и интенсивности исходящего и входящего трафиков. Она является также частью последовательности операций, выполняемых МСЭ для обеспечения безопасности внутренней сети от всех типов атак.

METHODS OF USING NETWORK ADDRESS TRANSLATION (NAT) TECHNOLOGY IN FIREWALLS

M.N. BOBOF

Abstract

Network Address Translation applied to the firewall which positioning between the internal and external networks. When a packet is leaving the trusted (internal) network, NAT translates the local source address to a global unique address and vice versa. This technology applied to secure trusted network's internal addresses to prevent unauthorized user from gathering information about the structure of internal network and the intensity of the incoming and outgoing traffic.

Литература

1. *Олифер В.Г.*, *Олифер Н.А*. Компьютерные сети, принципы, технологии, протоколы // П., 2007.
2. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // Cisco press, Second Edition, 2008.
3. *Ray Blair, Arvind Durai*. Cisco Secure Firewall Services Module (FWSM) // Cisco press, Second Edition, 2009.
4. RFC 1631 – The IP Network Address Translator (NAT).
5. RFC 2663 – IP Network Address Translator (NAT) Terminology and Considerations.

УДК 621.391

КОРРЕКЦИЯ ОШИБОК ЦИКЛИЧЕСКИМИ КОДАМИ С ИСПОЛЬЗОВАНИЕМ СТИРАНИЙ

А.В. ШКИЛЕНОК

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Рассматривается возможность коррекции случайных и зависимых ошибок циклических кодов с использованием стираний. Применение стираний при коррекции ошибок позволяет исправить вдвое большее количество ошибок при тех же корректирующих способностях кода.

Ключевые слова: циклические коды, коррекция ошибок, стирания.

Введение

Одной из основных проблем в современных телекоммуникационных системах является повышение надежности передачи информации и помехоустойчивости систем и сетей связи. Среди множества методов борьбы с ошибками при передаче данных наибольшее распространение получило помехоустойчивое кодирование, позволяющее повысить качественные показатели работы систем связи. В цифровых системах широкое применение получили итеративные коды, однако их высокая избыточность влечет за собой сложные и вычислительно трудоемкие алгоритмы их декодирования, что нередко является преградой на пути их использования в некоторых системах. В работе [1] при декодировании итеративных кодов предложено использовать метод коррекции ошибок с использованием стираний, что позволяет многократно увеличить количество исправляемых ошибок, не увеличивая длины и корректирующих способностей исходных кодов. Так как в качестве исходных кодов в итеративных могут использоваться и линейные блоковые, то весьма вероятно, что те же методы могут быть применены и при обработке циклических блочных кодов.

Важным моментом при декодировании кодов является наличие информации о структуре и количестве исправляемых ошибок в принимаемой кодовой последовательности. При наличии информации о местоположении неверно принятых символов их можно стереть, а потом применить метод исправления ошибок со стираниями, что позволит вдвое увеличить корректирующие способности кода, не изменяя при этом его параметров (длины, скорости и т.д.).

При таком подходе можно с достаточно высокой степенью вероятности утверждать об эффективности применения при декодировании циклических блоковых кодов тех же методов, что и при декодировании итеративных кодов, поскольку это дает принципиально новые возможности для повышении надежности передачи информации в каналах связи с высокой нестабильностью помех, универсальность в применении различных типов помехоустойчивых кодов для при решении одних и тех же задач, расширяет сферы применения данного типа кодов.

Коррекция случайных и зависимых ошибок при декодировании циклических кодов со стираниями

В работе [2] приводятся алгоритм и метод декодирования, использующие стирания при исправлении случайных ошибок. В работе [3] показано, что применяя классификацию ошибок, возможно многократно сократить количество анализируемых селектором комбинаций и уменьшить сложность декодера БЧХ-кодов. Согласно классификации ошибок все однократные зависимые ошибки являются типичными, поэтому все они могут корректироваться как частный случай независимых многократных ошибок. Применяя дополнительно к этому исправление ошибок со стираниями корректирующие способности кода можно дополнительно повысить.

Под стиранием понимаются искаженные символы, местоположение которых известно при декодировании, но неизвестно их истинное состояние. Эта дополнительная информация позволяет исправлять t ошибок и ρ стираний кодом, у которого:

$$d \geq 2t + \rho + 1. \qquad (1)$$

Например, код с $d = 7$ позволяет корректировать две ошибки и два стирания, одну ошибку и четыре стирания или шесть стираний. Как следует из (1) введение стираний, по сравнению с исправлением только ошибок, обладает тем преимуществом, что исправление ошибок требует вдвое больше усилий (и избыточности), чем исправление стираний, поскольку позиции стираний известны декодеру. Иными словами, информация о местоположении стертых символов позволяет в два раза повысить эффективность использования одного и того же кода по сравнению с обычным исправлением ошибок [4–7].

Известен простой метод исправления стираний с помощью линейного кода: стертые символы заменяются нулями, и вычисляется синдром. Если вычисленный синдром равен нулю, то принимается что, все стертые символы равны нулю. Если синдром не равен нулю, то один из стертых символов заменяется единицей и снова вычисляется синдром. В результате чего можно найти вектор согласования состояний стираний с переданными словами. Эта процедура повторяется до тех пор, пока соответствующий синдром не будет равен нулю.

Очевидно, что такой переборный метод исправления стираний требует больших временных затрат. В общем случае, для коррекции ρ стираний необходимо выполнять в худшем случае 2^{ρ} вычислений синдромов (на каждое вычисление синдрома также требуются временные затраты), поэтому данный декодер будет иметь низкое быстродействие. Этот недостаток обусловлен тем, что каждый раз необходимо вычислить синдром по правильным значениям принятых символов и подставляемых значений стираний и при этом не используется вычисленный синдром на предыдущем этапе.

При коррекции многократных ошибок возникает так называемая «проблема селектора», а при обнаружении ошибок такая проблема не возникает. Если использовать идентификацию ошибок, при которой ошибки обнаруживаются и определяется кратность произошедших ошибок, то можно выбрать эффективный алгоритм обработки: вначале осуществляется коррекция ошибок малой кратности, отказ от декодирования или установление местоположения стираний, которые затем корректируются как стирания. Это позволяет упростить реализацию декодера.

Многократные стирания (или стирания и ошибки) могут исправляться циклическими кодами следующим образом. Вначале заменяются все стертые символы нулями, и декодируется полученное слово с использованием стандартного алгоритма декодирования циклических кодов для коррекции только ошибок, и получается кодовое слово $A_0(x)$. Затем снова заменяются все стертые символы единицами, и осуществляется подобное декодирование и получается кодовое слово $A_1(x)$. Наконец выбирается из $A_0(x)$ и $A_1(x)$ в качестве результата декодирования кодовое слово, в котором было исправлено меньшее число ошибок в нестертых позициях [6, 7]. При этом любая допустимая по условию (1.1) комбинация стираний и ошибок исправляется за две попытки исправления только ошибок. Это значит, что рассмотренный метод исправления стираний циклическими кодами требует аппаратных и временных затрат вдвое больше, чем исправление только ошибок. Кроме того, при коррекции многократных стираний необходимо применить код с большим кодовым расстоянием, что по рассмотренному методу приводит к

коррекции многократных ошибок, и снова появляется проблема селектора. При исправлении только стираний (без ошибок) алгоритм декодирования упрощается. При этом стертые символы заменяются нулями, и вычисляется синдром. Если вычисленный синдром равен нулю, то принимается что, все стертые символы равны нулю. Если синдром не равен нулю, то один из стертых символов заменяется единицей и снова вычисляется синдром. В результате можно найти истинные состояния стираний. Эта процедура повторяется до тех пор, пока соответствующий синдром не будет равен нулю.

Таким образом, для коррекции ошибок циклическими кодами с использованием стираний необходимо применение двухэтапного метода декодирования:

- обнаружение ошибок и коррекция (коррекция ошибок малой кратности);
- стирание некорректируемых ошибок и коррекция стираний этим же кодом.

Декодер однократных стираний (в том числе пакетных и модульных) будет по своей структуре аналогичен декодеру, корректирующему однократные ошибки, за исключением добавления блока формирования вектора согласований стираний.

Для исправления многократных стираний потребуется дополнительно учитывать нетипичные векторы ошибок согласно классификации.

Быстродействие декодера можно увеличить, если при коррекции стираний перейти к параллельному вычислению векторов согласования стираний и формированию векторов ошибок (иначе придется многократно «прогонять» все содержимое регистра, что приводит к большим временным задержкам). При этом следует не забывать об обязательном наличии цепи обратной связи к БВС для модификации синдрома.

Общее правило декодирования циклических кодов с использованием стираний выглядит следующим образом:

1. Вычисление синдрома;
2. Коррекция корректируемых ошибок или идентификация некорректируемых;
3. Стирание позиций символов, идентифицированных, как ошибочные, но некорректируемые;
4. Поиск вектора согласования стираний;
5. Коррекция стираний;
6. Если комбинация неисправимая – отказ от декодирования.

По синдрому образующего вектора ошибок можно определить подмножество (подкласс) ошибок, а соответственно их кратность и местоположение. Для этого известный декодер классифицированных ошибок требуется дополнить третьим регистром с сумматорами по модулю два для параллельного исправления. При параллельном исправлении стираний возможно получение вектора согласования аналогичным образом, как и у линейных блоковых кодов. Задача нахождения вектора согласования выбранного значения состояния стираний с переданными является трудоемкой задачей. Однако ее можно упростить, если сопоставить каждому вектору согласования ω соответствующий синдром S и по совпадению вычисленного синдрома S с сопоставляемым находить соответствующий вектор ошибок.

Общее количество тактов на декодирование и коррекцию ошибок составляет $(2n\text{-}1)$ на вычисление синдрома и n тактов на исправление стираний.

Преимуществом перед классическим декодером со стираниями будет являться уменьшение задержек при вычислении синдромов ошибок, так как вычисление синдрома будет происходить на каждом этапе исправлений лишь однократно.

Метод исправления стираний на основе нахождения векторов согласования стираний позволяет предложить декодер с приемлемой сложностью и быстродействием. Важным моментом является возможность реализации блочной структуры декодера на ПЗУ и ПЛИС, которая затем легко наращивается модульным путем при помощи увеличения числа однотипных функциональных блоков, что позволит сохранить высокое быстродействие за счет однородности структуры. При коррекции однократных модульных и пакетных стираний объем ПЗУ можно уменьшить за счет хранения только ошибочных модулей, а не всех векторов ошибок.

Известен метод коррекции ошибок с использованием стираний, подробно рассмотренный в [2]. Известно, что для двоичных кодов ошибке в i-ой позиции кодового слова соответствует синдром, образованный i-ым столбцом проверочной матрицы, а в случае наличия

многократных ошибок синдром равен сумме синдромов, образованных теми столбцами, где произошли ошибки. Это можно использовать для разработки декодера циклических кодов с исправлением стираний.

Вначале, согласно символам принятого слова A_n^* вычисляется синдром S:

$$S = A_n^* \cdot H^T. \qquad (2)$$

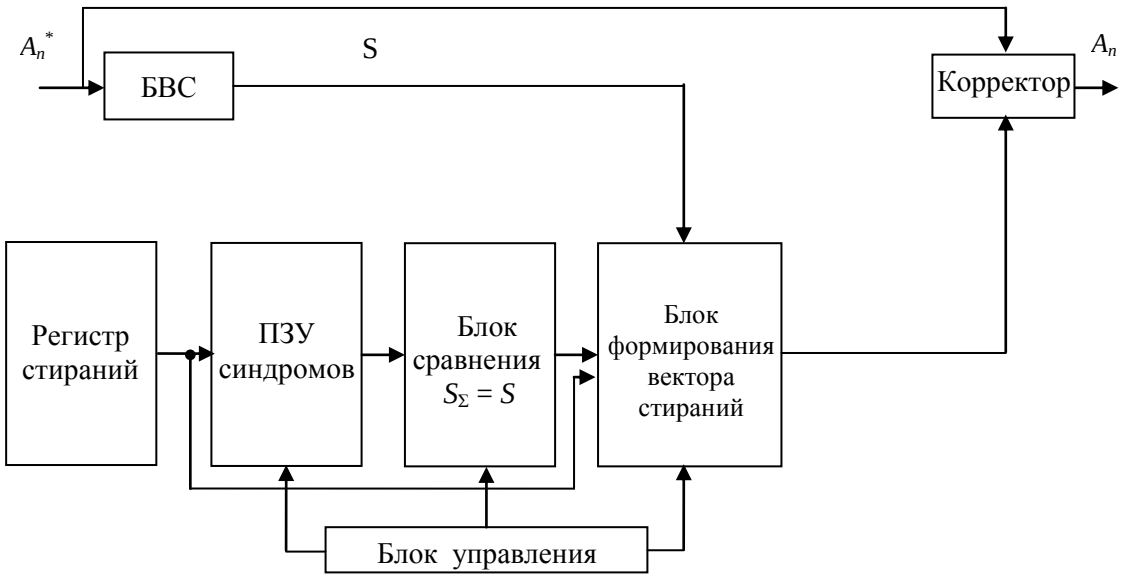
После этого, состояние в стертых разрядах заменяется всеми возможными комбинациями, и вычисляются синдромы S_Σ, соответствующие векторам со значениями нестертых символов, равными нулю. Сравнивая S с S_Σ можно найти вектор ошибки и выполнить исправление стираний.

Вышеописанный алгоритм позволяет уменьшить задержку в силу уменьшения задержек при вычислении синдромов, но тем не менее, это тоже переборный метод. Отметим, что в вышеописанном алгоритме столбцы проверочной матрицы, соответствующие нестертым позициям принятого слова не влияют на значение синдрома S, следовательно, при вычислении синдрома S можно пренебречь этими столбцами.

Рассмотрим более эффективный метод исправления стираний основанный на использовании вычисленного на первоначальном этапе синдрома S, известных позиций стираний, а следовательно и составляющих одиночных синдромов. В соответствии с позициями стертых разрядов составляется подматрица стираний, которая содержит столбцы проверочной матрицы кода H с номером, равным номеру позиции стирания. Обозначим вектор согласования состояний стираний ω – вектор строки с ρ элементами, i-й элемент соответствует i-ой слева стертой позиции и равен нулю, если значение этой позиции у принятого слова совпадает с правильным значением кодового слова и равен единице в противном случае. Вектор согласования со стираниями ω, равен вектору ошибок e, который имеет единичные значения в стертых позициях и значения нуля в остальных позициях, например, $e = (00\omega_1 0 \ldots 0 \omega_2 \ldots \omega_\rho 0 \ldots 0)$.

Согласно принятому слову вычисляется синдром S_Σ. Если $S_\Sigma = 0$, то вектор согласования состояний стираний равен нулю, в принятом слове нет ошибок и все стертые разряды согласованы с их значениями. Когда $S_\Sigma \neq 0$ производится выбор из ПЗУ соответствующего вектора согласования и формируется вектор ошибки, который подается на блок коррекции для исправления ошибок в принятой кодовой комбинации.

Структурная схема декодера циклического кода со стираниями представлена на рисунке.



Структурная схема декодера циклического кода со стираниями

Предложенный декодер может быть достаточно просто реализован аппаратно с применением ПЗУ или ПЛИС для нахождения всех одиночных синдромов стертых позиций и

их всевозможных сумм, блока совпадения и блока формирования вектора ошибок по вектору ω. Декодер по предложенному алгоритму будет обладать высоким быстродействием благодаря вычислению синдрома только один раз.

Выводы

Проведенные исследования показали возможность использования стираний при коррекции случайных и зависимых ошибок циклическими кодами Предложена структурная схема декодера циклических кодов с использованием стираний. Исправление многократных случайных и зависимых ошибок также возможно, однако это значительно увеличивает количество анализируемых комбинаций и, соответственно, требуемый объем памяти для хранения синдромов ошибок и векторов согласования. Полученные результаты подтверждают возможность использования при коррекции многократных случайных, пакетов и модулей ошибок циклическими кодами в режиме исправления со стираниями.

ERROR CORRECTING CYCLIC CODES WITH USING ERASURES

A.V. SHKILENOK

Abstract

Considered ability of correct dependent and independent errors by cyclic codes with using erasures. Applying erasure with correction errors let correct double amount of errors with the same correcting abilities of codes.

Литература

1. *Фам, Хак Хоан* // Докл. БГУИР. 2008. № 1. 141-146.
2. *Конопелько В.К., Липницкий В.А., Дворников В.Д. и др.* Теория прикладного кодирования: Учебное пособие. М., 2004.
3. *Шкиленок А.В. Конопелько В.К* // Докл. БГУИР, 2007. №2 (18), С. 12 – 18.
4. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки. М., 1986.
5. *Вернер М.* Основы кодирования. М., 2006.
6. *Кларк, Дж. мл.* Кодирование с исправлением ошибок в системах цифровой связи. М., 1987.
7. *Морелос–Сарагоса Р.* Искусство помехоустойчивого кодирования. М., 2005.

УДК 621.391.(075.8)

ДЕКОДИРОВАНИЕ КРАТНЫХ ОШИБОК НА ОСНОВЕ ЦИКЛОТОМИЧЕСКОГО СЖАТИЯ НОРМ СИНДРОМОВ

А.В.КУРИЛОВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Работа посвящена совершенствованию норменных методов коррекции ошибок для семейства БЧХ-кодов. Разрабатывается метод сжатия норм синдромов с помощью циклотомических подстановок. Переход к G-орбитам в примитивных БЧХ-кодах позволяет дополнительно сократить в $Log_2 n$ раз количество селектируемых Г-орбит.

Ключевые слова: синдром ошибок, норма синдрома, автоморфизм кода, циклическая подстановка, циклотомическая подстановка, БЧХ-код, декодер.

Введение

На рубеже 20 – 21 веков белорусской школой кодировщиков разработана теория норм синдромов – новое направление в теории и практике помехоустойчивого кодирования. Основным ее практическим результатом явилась серия норменных перестановочных методов коррекции кратных ошибок для широкого семейства циклических кодов, в частности, для семейства кодов Боуза-Чоудхури-Хоквингема (БЧХ-кодов) [1, 2]. Норменные методы отличают сокращение в n раз (n – длина кода) количества селектируемых комбинаций, конструктивная возможность исчерпания избыточности кодов, однородность структуры декодирующих схем.

Интенсивный рост объемов информации в современных инфокоммуникационных системах предъявляет жесткие требования к декодерам, прямым следствием которых является необходимость увеличения длин помехоустойчивых кодов и кратностей корректируемых ошибок. Эти требования приводят к необходимости дальнейшей работы по развитию теории норм синдромов и норменных методов коррекции ошибок. В [3] предложен оригинальный метод сжатия норм синдромов путем отображения векторов-ошибок в класс векторов-ошибок большей кратности. В данной работе рассматривается сжатие норм синдромов последовательным применением циклотомических подстановок.

Циклические и циклотомические подстановки принадлежат группам автоморфизмов многих циклических кодов, в том числе кодов семейства БЧХ [2, 4]. В данной работе на основе изученного влияния циклотомических подстановок на синдромы ошибок и нормы синдромов предложен альтернативный метод сжатия норм синдромов. Совместная группа G циклических и циклотомических подстановок разбивает корректируемую совокупность векторов-ошибок на непересекающиеся классы – G-орбиты. При этом G-орбиты состоят из Г-орбит. В примитивных БЧХ-кодах в подавляющем большинстве случаев G-орбита содержит $Log_2 n$ Г-орбит. Традиционные норменные методы требуют селекции всего многообразия Г-орбит корректируемой совокупности (что как известно в n раз меньше количества синдромов исправляемых векторов-ошибок). Предлагается модификация норменного метода, согласно которой следует селектировать только образующие G-орбит. В таком случае по вычисленным синдрому и норме синдрома определяем G-орбиту, содержащую искомую вектор-ошибку, затем осуществляем поиск вектора-ошибки внутри G-орбиты. Такой метод дополнительно

сокращает в $Log_2 n$ раз мощность селектируемой совокупности норм синдромов, что в конечном итоге соответственно уменьшает сложность декодирующих устройств.

Действие циклотомических подстановок на пространстве векторов-ошибок двоичных кодов

Определим на множестве $T = \{0,1,2,...,n-1\}$ преобразование φ по следующему правилу: для каждого $i \in T$ $\varphi(i) = \overline{2i}$ – элемент множества T, равный $2i$, если $2i < n$, и равный $2i - n$, если $2i \geq n$. Известно [2], что отображение φ является биекцией множества T тогда и только тогда, когда n нечетно. В дальнейшем $n = 2l + 1$ – нечётно. Существует наименьшее натуральное m с условием: $2^m - 1 = nq$, то есть n делит $2^m - 1$. Тогда циклическая группа Ф, порожденная степенями φ, конечна и имеет порядок m.

Группа Ф действует на пространстве ошибок E_n любого двоичного линейного кода, переставляя координаты векторов-ошибок в соответствии с указанным выше правилом действия на их номера, образующие множество T. Действия φ и ее степеней на $i-$ элемент множества $T-$ образуют циклотомический класс $i, 2i, 2^2 i, \cdots, 2^{m-1} i$ по модулю n [3]. Поэтому подстановки $\varphi, \varphi^2, \cdots, \varphi^m$ – называются циклотомическими. Действие подстановок $\varphi, \varphi^2, \cdots, \varphi^m$ на векторы пространства E_7 иллюстрирует рис. 1.

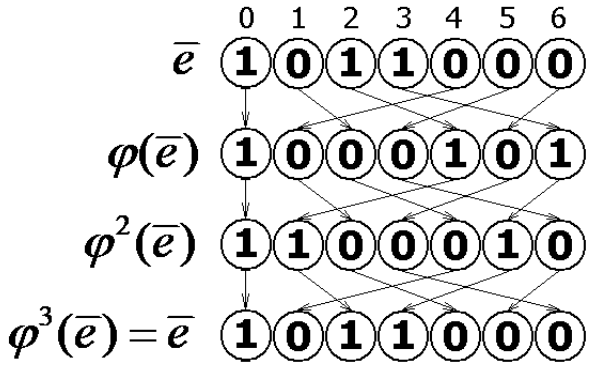


Рис. 1. Действие циклотомической подстановки φ и ее степеней в пространстве E_7 на вектор $\bar{e} = (1011000)$

Подстановки $\varphi, \sigma \in S_n$ для циклической подстановки σ на множестве T взаимосвязаны: для произвольного $\bar{e} \in E_n$ $\varphi\ \sigma\ \bar{e}\ = \sigma^2\ \varphi\ \bar{e}$ [2]. Они порождают некоммутативную группу G подстановок порядка mn.

Два вектора $\bar{f}$ и $\bar{g}$ из E_n называются G – эквивалентными, если найдется подстановка $\tau = \varphi^j \sigma^i \in \mathrm{G}$, такая, что $\bar{g} = \tau\ \bar{f}$. G – орбитой называется совокупность всех попарно G-эквивалентных между собой векторов-ошибок из E_n. Если $\bar{e}$ – фиксированный вектор данной G – орбиты, то G – орбиту с вектором $\bar{e}$ будем обозначать через $<\bar{e}>_G$.

Пусть $<\bar{e}>$ – Г-орбита, порожденная вектором $\bar{e} \in E_n$ [2]. Тогда $\varphi<\bar{e}>$ также является Г-орбитой. Поэтому всякая G-орбита имеет следующую структуру: $<\bar{e}>_G = <\bar{e}>, \varphi<\bar{e}>, \varphi^2<\bar{e}>, \ldots, \varphi^{\mu-1}<\bar{e}>$, где $\varphi^\mu <\bar{e}> = <\bar{e}>$, $\mu = m$ или делит m.

В табл. 1 приведены значения количества векторов-ошибок весом 2 – 4, их Г-орбит и G-орбит в примитивных БЧХ-кодах длиной в диапазоне от 15 до 1023.

Таблица 1. **Количество ошибок данного веса, их Г-орбит и G-орбит в зависимости от n**

Вес ω	Количество	Длина кода, n						
		15	31	63	127	255	511	1023
2	Ошибок	105	465	1 953	8 001	32 385	130 305	522 753
	Г-орбит	7	15	31	63	127	255	511
	G-орбит	3	3	7	9	16	29	52
3	Ошибок	455	4495	3 9711	333375	2731135	22108415	177910271
	Г-орбит	31	145	631	2625	10712	43265	173911
	G-орбит	10	29	106	375	214	4808	17395
4	Ошибок	13655	31465	595665	10334625	1,72E+08	2,81E+09	4,54E+10
	Г-орбит	91	1015	9455	81375	674751	5494655	44347135
	G-орбит	24	203	1577	11625	84345	610519	443474

Табл. 1 демонстрирует, что количество Г-орбит в n раз меньше количества векторов-ошибок данного веса, а количество G-орбит в $Log_2 n$ раз меньше числа составляющих их Г-орбит.

Влияние циклотомических подстановок на синдромы и нормы синдромов векторов-ошибок

Пусть $S\ \bar{e}\ = s_1, s_2, ..., s_{\delta-1}$ - синдром вектора-ошибки $\bar{e}$ в БЧХ коде С с проверочной матрицей $H=[\alpha^{bi}, \alpha^{(b+1)i}, ..., \beta^{(b+\delta-2)i}]^T$. Тогда синдром $S\ \varphi\ \bar{e}\ = s_1^2, s_2^2, ..., s_{\delta-1}^2$ [2]. Отсюда и из определения компонент нормы синдрома [2] вытекает, что компоненты нормы синдрома $N\ S\ \varphi\ \bar{e}$, преобразуются аналогично – возводятся в квадрат как элементы поля Галуа.

В табл. 2 приведен список G-орбит и составляющих их Г-орбит векторов-ошибок весом 2 в пространстве E_{31}, синдромов образующих и норм синдромов в БЧХ-коде C_5 над полем $GF(32)$ с примитивным элементом α – корнем полинома $x^5 + x^2 + 1$.

Каждая G-орбита в табл. 2 является полной – содержит максимально возможное количество Г-орбит, при этом построена из Г-орбит по циклу: следующая Г-орбита есть образ предыдущей под действием φ, последняя при этом переходит в первую. Аналогично выбраны и образующие Г-орбит. Поэтому компоненты синдрома каждой следующей образующей являются квадратами соответствующих компонент синдрома предыдущей образующей. Такая же взаимосвязь и норм синдромов внутри G-орбит.

Таким образом, зная образующую G-орбиты, а также ее синдром, можно однозначно восстановить элементы всей G-орбиты и синдромы всех ее векторов-ошибок.

Таблица 2. **Структура G-орбит векторов-ошибок весом 2 в пространстве** E_{31}

№ п/п G-орбиты	G-орбита $<\bar{e}>_G$	Образующая Г-орбиты $<\bar{e}>$	Показатели ($\deg S_1$, $\deg S_2$) компонент синдрома $S\ \bar{e}\ =(s_1,s_2)$	Показатель нормы degN(S($\bar{e}$))
1	$<\ 0,1\ >_G$	(0,1)	(18,29)	6
		(0,2)	(5,27)	12
		(0,4)	(10,23)	24
		(0,8)	(20,15)	17
		(0,16)	(9,30)	3
2	$<\ 0,3\ >_G$	(0,3)	(29,16)	22
		(0,6)	(27,1)	13
		(0,12)	(23,2)	26
		(0,24)	(15,4)	21
		(0,17)	(30,8)	11
3	$<\ 0,5\ >_G$	(0,5)	(2,24)	18
		(0,10)	(4,17)	5
		(0,20)	(8,3)	10
		(0,9)	(16,6)	20
		(0,13)	(14,20)	9

Норменный метод коррекции ошибок на основе циклотомических подстановок

Предложенная классификация векторов-ошибок позволяет сформулировать норменный перестановочный метод коррекции ошибок в БЧХ-кодах на основе циклотомических подстановок.

Предварительно составляем список 1 образующих $\bar{g}_i$ из совокупности $K=\ G_1,\ldots,G_t$ G-орбит корректируемых векторов-ошибок, список 2 синдромов $S\ \bar{g}_i$ и список 3 норм синдромов $\bar{N}_i = N\ \ S\ \ \bar{g}_i$ или показателей $d_i = \deg N_i$.

Предлагаемый метод можно сформулировать следующим образом.

Приняв сообщение $\bar{x}_i$, вычисляем его синдром ошибок $S\ \ \bar{x}\ =\alpha^i$.

Вычисляем текущую норму $\bar{N}_{тек} = N\ \ S\ \ \bar{x}$ (или показатель $\deg\ \ N\ \ S\ \ \bar{x}$.

В счётчике итераций алгоритма записываем «0».

Текущую норму сравниваем с множеством $\bar{N}_1,\ldots,\bar{N}_t$ третьего списка. Если $N=\bar{N}_i$, то переходим к этапу 4. Если же $N\notin\ \bar{N}_1,\ldots,\bar{N}_t$, , то переходим к этапу 5.

По текущему значению синдрома в Г-орбите $<g_i>$ с нормой $\bar{N}_i$ по одному из вариантов известного норменного алгоритма (см. [2], раздел 5.1) находим вектор-ошибку $\bar{e}_{тек}$. Если в счётчике записано значение «0», то переходим к последнему - седьмому этапу алгоритма. Если в счётчике записано ненулевое значение, то переходим к шестому этапу.

Вычисляем квадрат текущей нормы, а с ним и квадраты компонент синдрома. Значение счётчика итераций увеличиваем на 1. С полученными текущими значениями нормы и синдрома возвращаемся к этапу 3.

Если в счётчике записано число $k,\ 1\le k\le m-1,$ то находим истинный вектор ошибок по формуле $\bar{e}=\varphi^{m-k}(\bar{e}_{тек})$ и переходим к седьмому этапу алгоритма.

Находим истинное сообщение $\bar{c}=\bar{x}+\bar{e}$.

Техническая реализация данного метода может иметь различные варианты в зависимости от применяемых средств и схем декодеров. Наиболее естественной, является схема декодера, представленная на рис. 2 для коррекции ошибок в (21, 31)-БЧХ-коде C_5, исправляющем двойные ошибки. Необходимые данные представлены в табл. 2. Здесь синдром S поступает через мультиплексоры M_i, M_j на логическую матрицу ЛМ1, выделяющую только три фиксированные нормы синдрома N_1, N_2, N_3. Если на выходе ЛМ1 присутствует логический "0", то счетчик Cr переходит из состояния (0,0,...,0) в состояние (1,0,...,0). Далее, декодер переходит к реализации п. 4 алгоритма. При наличии логической "1" на выходе ЛМ1 – к п. 5 алгоритма.

В двух блоках умножения БУ1, БУ2 последовательно производится параллельное возведение в квадрат компонент синдрома s_1 и s_2 как элементов поля Галуа. Полученные значения квадратов поочередно опрашиваются через мультиплексоры M_i, M_j под управлением выходного кода счетчика. Данная операция по сути дела осуществляет последовательную перестановку образующих векторов Г-орбит ошибок.

При логическом "1" на выходе ЛМ1 счетчик останавливается, фиксируя тем самым код перестановки текущей нормы синдрома до одной из выбранных норм N_1, N_2, N_3. Компоненты вычисленного синдрома $S^* = (s_1^2, s_2^2)$ поступают на ЛМ2. На выходе ЛМ2 будет находиться вектор ошибок $\overline{e}_i^*$ из Г-орбиты J_i с нормой N_i, синдром которого равен S^*.

На седьмом этапе найденный вектор $\overline{e}_i^*$ поступает на блок обратной перестановки вектора ошибок (БОПВО) для нахождения истинного вектора ошибок $\overline{e}$. Это можно осуществить под управлением кода перестановки, хранимого в счетчике.

Реализация БОПВО сопряжена с определенными трудностями, поскольку необходимо реализовать не циклическую перестановку для вектора ошибок данной нормы N_i, а преобразование с изменением диаметра, полученного с ЛМ1 с нормой синдрома N_i. Зная степени i_T и i_0 синдромов можно определить, код сдвига $L_{сдв} = i_T - i_0$ для нормы N_i. В Величина сдвига не меняется под действием преобразований этапа 4 и, следовательно, остается одинаковой для всех рассматриваемых алгоритмом Г-орбит. Тогда по известному коду перестановки (а, значит, и по известной норме) можно сформировать образующий вектор ошибок и сдвинуть его в регистре сдвига на соответствующее число тактов, или же по адресу не сдвинутого вектора ошибок находить адреса текущего вектора ошибок.

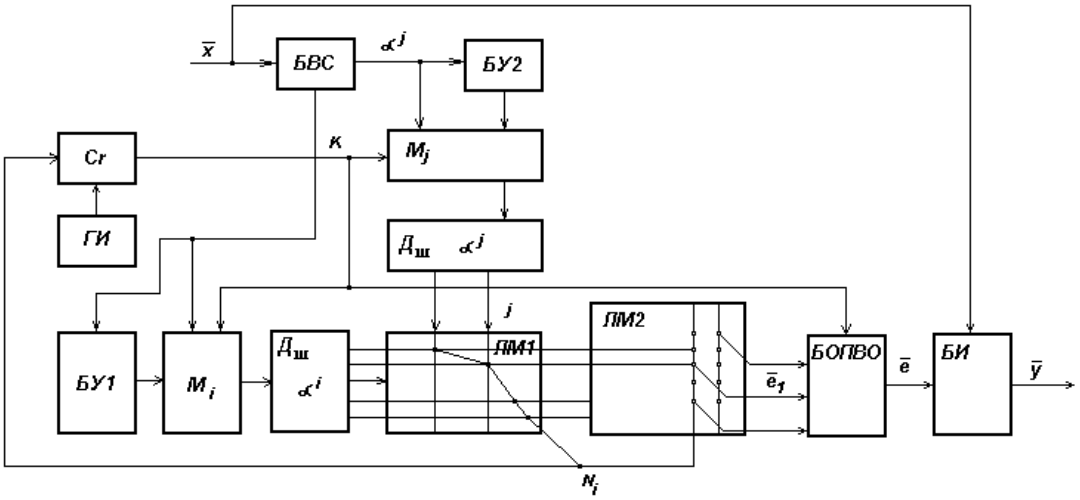


Рис. 2. Структурная схема декодера, реализующего метод циклотомического сдвига для t=3

Анализ затрат на реализацию метода показывает, что резкое сокращение аппаратурных затрат (например, для t=3 емкость ЛМ1 равна 3n, а ЛМ2 – 6n, то есть суммарная сложность равняется 9n) связано с увеличением числа тактов на перебор всех норм синдромов. Так при длине кода n=31 при t=3 в худшем случае требуется 161 такт (примерно 5n тактов) на декодирование.

Заключение

В работе исследован норменный метод коррекции ошибок БЧХ-кодами на основе циклотомических перестановок. Этот метод позволяет существенно сократить множество селектируемых норм синдромов (в $Log_2 n$ раз для примитивных БЧХ-кодов, где $n-$ длина кода). Предложена реализация метода декодером на логических матрицах или на программируемых логических интегральных схемах.

DECODING OF MULTIPLE ERRORS ON THE BASIS OF CYCLOTOMIC COMPRESSION OF NORMS OF SYNDROMES

A.V. KURYLOVICH

Abstract

Work is devoted perfection norm methods of correction of errors for family of BCHH-CODES. The method of compression of norms of syndromes with the help cyclotomic substitutions is developed. Transition to G-orbits in primitive BCHH-CODES allows to reduce in addition in $Log_2 n$ time quantity selected G-orbits.

Литература

1. *Конопелько В.К., Липницкий В.А.* Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов. М, 2004.
2. *Липницкий В.А., Конопелько В.К.* Норменное декодирование помехоустойчивых кодов и алгебраические уравнения. Мн., 2007.
3. *Курилович А.В., Конопелько В.К., Липницкий В.А.* // Докл. БГУИР, 2005. № 6. 28 – 30.
4. *Мак-Вильямс, Ф.Дж.* Теория кодов, исправляющих ошибки. М., 1979.

УДК 621.391.(075.8)

ПОИСК ОБРАЗОВ ДВУМЕРНЫХ ЗАВИСИМЫХ ОШИБОК

О.Г.СМОЛЯКОВА, Е.Г. МАКЕЙЧИК, И.В. КОНОПЕЛЬКО

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Рассматривается классификация образов зависимых двумерных ошибок. Определяются образующие вектора зависимых ошибок. Предлагается метод и алгоритм формирования библиотек пакетных ошибок. Определяются образы модульных ошибок.

Ключевые слова: двумерные ошибки, вектор ошибки, пакетные и модульные ошибки.

Введение

При применении двухмерного кодирования кодовое слово $A_{\text{дв}}$ представляет собой таблицу, состоящую из X строк и Y столбцов. Ошибка, которая возникает в таком кодовом слове, обладает двумя параметрами – номером строки x и номером столбца y, в котором она находится. Однако, при больших длинах кодовых слов $n=n_1 \cdot n_2$, существуют случаи, когда строка или столбец двухмерного кодового слова $A_{\text{дв}}$ не содержат ошибочных символов, тогда образ двухмерной ошибки $ve_{\text{дв}}(A_{\text{дв}})$ слова $A_{\text{дв}}$ образуется путем вычеркивания из исходного слова безошибочных строк и столбцов. Все возможные образы случайных ошибок кратности t представляют собой полное множество перестановок t ошибочных символов в таблице, размерностью txt.

Пакетную ошибку можно представить как частных случай случайной ошибки, а модульная ошибка является частным случаем пакетной ошибки, часто её называют фазированным пакетом ошибок. Так как для поиска образов случайных ошибок используется образующие вектора случайной ошибки, представляющий собой множество одномерных векторов ошибок размерностью txt с кратностью ошибок t, то, следовательно, для поиска образов двумерных пакетных/модульных ошибок можно воспользоваться этим множеством, исключив вектора, которые не образуют искомых пакетных/модульных ошибок. В статье предлагается метод поиска и определения образов двумерных зависимых ошибок с помощью образующих векторов пакетных/модульных ошибок.

Образующие вектора зависимых ошибок

Образующим вектором $e^{P}_{\text{обр}}$ пакетной ошибки называется образующий вектор случайной ошибки, зависящий от кратности ошибки t и содержащий t_n пакетов длины p, а образующим вектором $e^{M}_{\text{обр}}$ модульной ошибки называется образующий вектор пакетной ошибки содержащий t_b пакетов длины b. Вектора $e^{P}_{\text{обр}}$, $e^{M}_{\text{обр}}$ зависят от кратности ошибок t. На рис. 1 показаны образующие вектора пакетной и модульной ошибок.

Для поиска и определения образов пакетных ошибок необходимо проанализировать образующие вектора пакетной ошибки разной кратности. Например, для формирования библиотеки образов пакетных ошибок кратности $t_{\text{n}}=2$ и длины $t=3$. Необходимо проанализировать образующие вектора пакетных ошибок кратности 4, 5 и 6.

Образующие вектора пакетных ошибок можно представить в виде множеств, содержащих вектора определенной кратности (рис. 2), а процедуру вычисления всех необходимых для анализа векторов как отбор определенных подмножеств и вычеркивание из

них тех векторов, которые не содержат t_n пакетов длины p. Аналогичным образом определяется процедура нахождения образующих векторов для модульных ошибок.

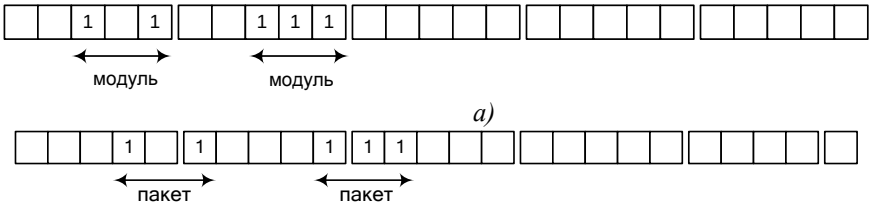


Рис. 1. Образующие вектора ошибок, t=5: *а* – $e^{P}_{обр}$ модульной ошибки; *б* – $e^{M}_{обр}$ пакетной ошибки

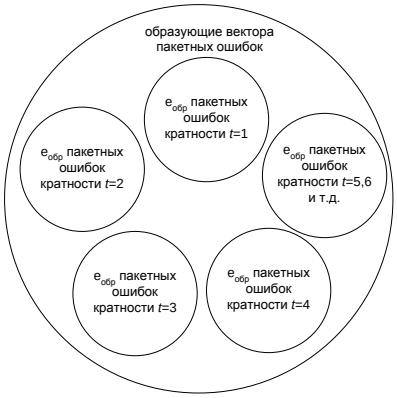


Рис. 2. Множество образующих векторов пакетных ошибок

Чтобы выделить среди всех образов случайных ошибок только пакетные, необходимо:

1. Сгенерировать образующие векторов $e_{обр}$ случайной ошибки кратности $t=p \cdot t_n$, где t_n – кратность пакета ошибок, представляющие собой все возможное перестановки из t на длине txt.

2. Определить, содержит ли вектор $e_{обр}$ только t_n пакетов длины p: если содержит – то вектор включается в множество образующих векторов пакетных ошибок, в противном случае – вектор исключается.

Алгоритм реализации пункта 1 метода генерации пакетов представлен на рис. 3, а пункта 2 – на рис. 4.

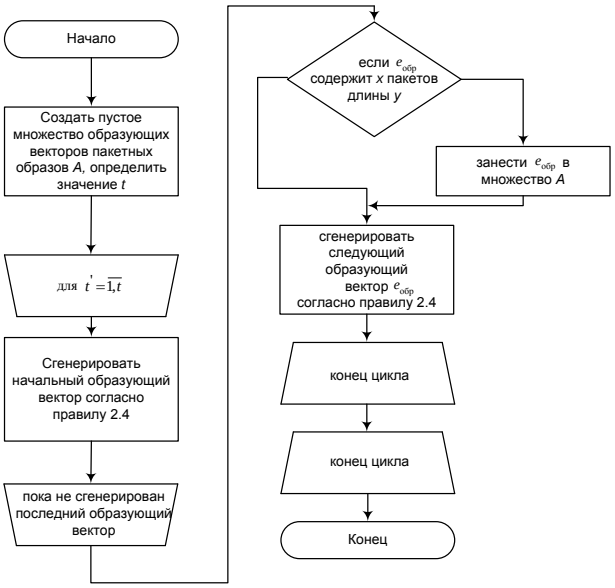


Рис. 3. Алгоритм реализации шага 1 метода генерации пакетов

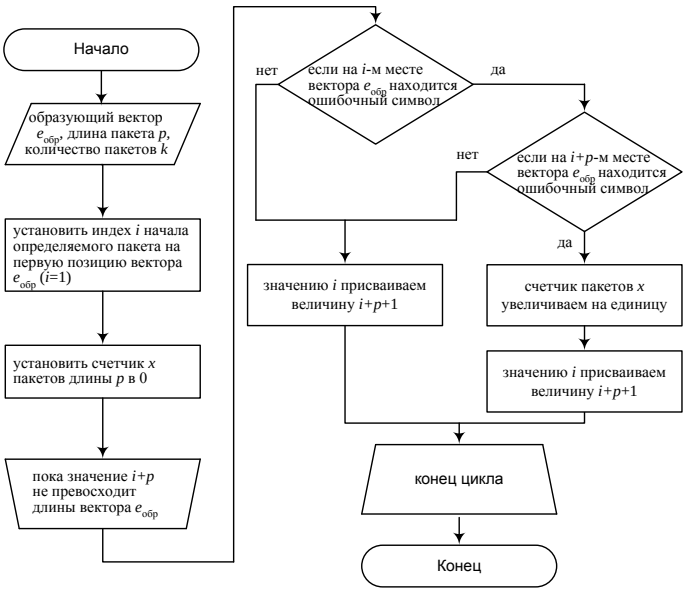


Рис. 4. Алгоритм реализации шага 2 метода генерации пакетов

С увеличением кратности корректируемой ошибки число образующих векторов ошибок, необходимых для анализа, также увеличивается (табл. 1). Анализ данных таблицы показывает, что число образующих векторов пакетных ошибок невелико и вычислительная сложность также не велика. Однако с увеличением величины кратности числа пакетов t_n растет и число образующих векторов пакетных ошибок, что для больших значений кратности ошибок приводит к проблеме вычислительной сложности.

Таблица 1. **Число анализируемых образующих векторов пакетных ошибок в зависимости от кратности ошибки при применении перестановочного метода формирования образующих векторов пакетных ошибок**

Кратность ошиб-ки t	Длина пакета p	Количество пакетов t_n	Число анализируемых $e_{обр}$, C_p	Кратность ошибки t	Длина пакета p	Количество пакетов t_n	Число анализируемых $e_{обр}$, C_p
2	2	1	3	6	2	1	35
3	2	1	8		2	2	561
	3	1	14		2	3	5456
4	2	1	15		3	1	68
	2	2	91		3	2	1984
	3	1	28		4	1	132
	4	1	52		5	1	256
	3	2	66		6	1	496
5	2	1	24		5	2	8316
	2	2	253		4	2	4785
	3	1	46		4	3	2925
	4	1	88		3	3	4060
	5	1	168				
	4	2	855				
	3	2	630				

Для снижения вычислительной сложности и увеличения быстродействия следует воспользоваться свойством позиционной модификации для формирования образующих векторов, приведенный ниже.

Свойство позиционной модификации. Образующий вектор пакетной ошибки содержит пакет ошибок либо целиком в одной строке таблицы или в двух строках (рис. 5).

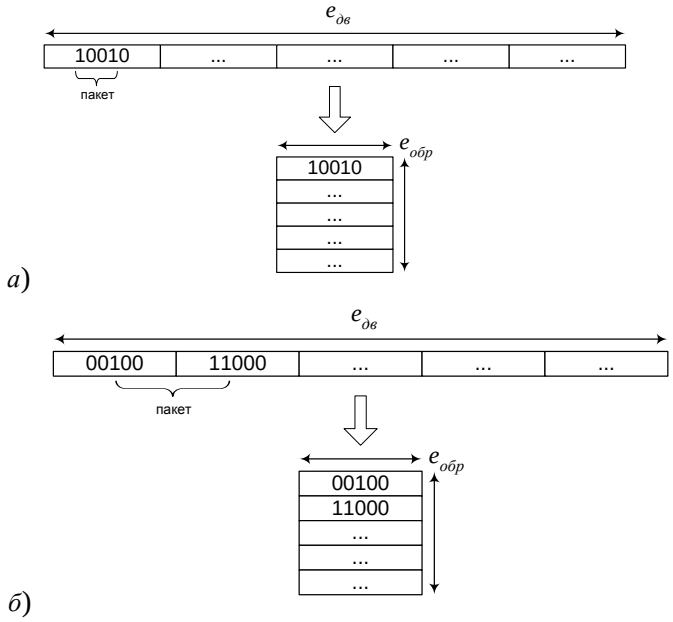


Рис. 5. Размещение пакета в образующем векторе ошибки:
а – пакет располагается в одной строке;
б - пакет располагается в двух строках

Отсюда, если вектор $e_{обр}$ содержит x пакетов, то они будут размещены максимум в $2*x$ строках.

Кроме того, если первый ошибочный символ образующего вектора пакетной ошибки $e_{обр}$ располагается на позиции с номером большим чем t, то генерируемый им образ ошибки будет одинаковым с образом, генерируемым вектором, у которого первый ошибочный символ располагается на позиции с номером меньшим t.

На основании этого предлагается *метод быстрого уменьшения числа образующих векторов* пакетных ошибок сущность состоит в том, что если первый ошибочный символ вектора $e_{обр}$ расположен на позиции с номером, большим t, то такой вектор из множества образующих векторов пакетных ошибок исключается.

Для формирования образующих векторов пакетных ошибок можно предложить *позиционный метод* сущность состоит в том, что если количество пакетов, необходимых для анализа равно t_n, кратность корректируемой ошибки t, p – длина пакета ($p<t$), то для генерации всех пакетных образов ошибок достаточно образующего вектора длиной $n_1'=2* t_n *t$.

Для реализации позиционного метода формирования образующих векторов пакетных ошибок используются следующие шаги:

1. Длина образующего вектора пакетной ошибки устанавливается равной $n_1'=2* t_n *t$

2. Генерируются все пакетные образующие вектора с кратностью исправляемой ошибки $t' = \overline{1,t}$.

Аналогичные подходы и реализации методов можно применить для поиска и сокращения числа образующих векторов модульных ошибок.

Коэффициент уменьшения количества образующих векторов пакетных ошибок при использовании быстрого и позиционного методов представлен в табл. 2, анализ данных которой показывает, что применение позиционного метода сжатия пакетных образующих

векторов эффективно при малом числе недлинных пакетов на длине образующего вектора пакетной ошибки.

Таблица 2. **Число образующих векторов пакетных ошибок при использовании быстрого и позиционного метода формирования**

Кратность ошибки t	Длина паке-та p	Коли-чество паке-тов t_n	Число векторов		Коэффициент уменьшения	
			быстрый метод, C_{p1}	позици-онный метод C_{p2}	C_p/C_{p1}	C_p/C_{p2}
2	2	1	3		1	
3	2	1	4		2	
	3	1	7		2	
4	2	1	5		3	
	2	2	47		1,94	
	3	1	9		3,11	
	4	1	17		3,06	
	3	2	38		1,74	
5	2	1	6		4	
	2	2	101	76	2,5	3,33
	3	1	11		4,18	
	4	1	21		4,19	
	5	1	41		4,1	
	4	2	400	275	2,13	3,11
	3	2	270	195	2,33	3,23
6	2	1	7		5	
	2	2	184	112	3,01	5
	2	3	2532		2,15	
	3	1	13		5,23	
	3	2	685	397	2,9	5
	4	1	25		5,28	
	5	1	49		5,22	
	6	1	97		5,11	
	5	2	3234	1650	2,57	5,04
	4	2	1749	957	2,73	5
	4	3	1595		1,83	
	3	3	2036		2	

Метод поиска образов зависимых ошибок

Формирующим вектором $e_{форм}$ образа ошибки является вектор, полученный из образующего вектора $e_{обр}$ путем вычеркивания безошибочных строк (блоков длины t). Группой образов называется множество формирующих векторов $e_{форм}$, количество строк которых одинаково. Очевидно, что количество групп, по которым распределяются формирующие

вектора ошибок, равно t, а количество блоков длиной y в каждой группе изменяется от 1 до t. Классом образов назовем множество формирующих векторов $e_{форм}$, являющихся циклическими сдвигами друг друга не содержащие нулевых блоков.

Распределение формирующих векторов по классам внутри группы позволит уменьшить вычислительную сложность при устранении избыточности библиотеки образов за счет уменьшения числа сравнений классов между собой. Причем для сравнения достаточно одного вектора, принадлежащего классу, так как остальные формируют тот же образ ошибки по определению.

Распределение формирующих векторов ошибок по группам и классам внутри группы для t=3 приведено на рис. 6.

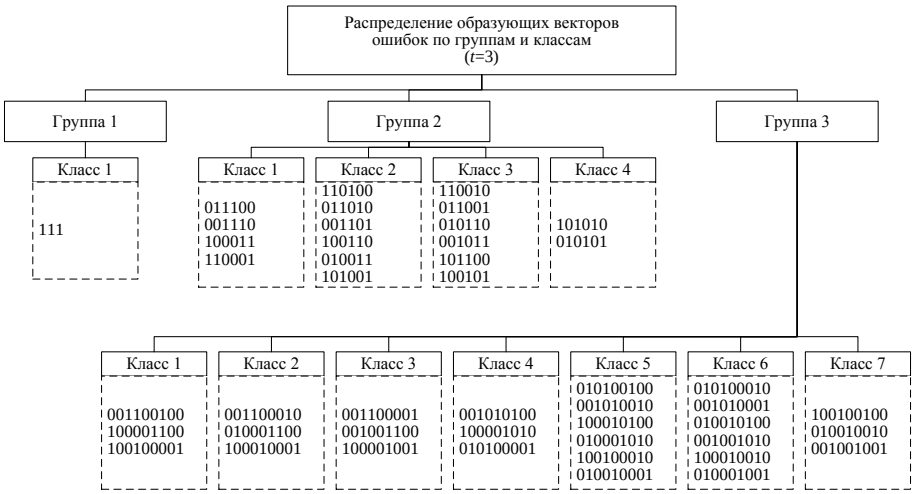


Рис. 6. Распределение образующих векторов ошибок по классам внутри группы

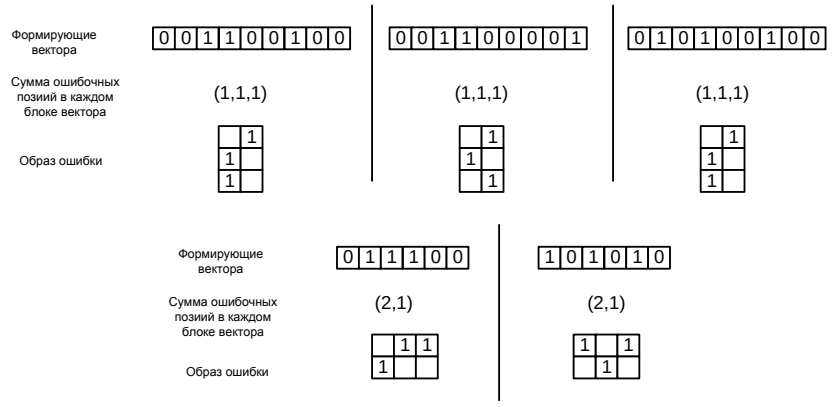
Вектора из разных групп формируют различные образы ошибок, а вектора из одной группы, но разных классов могут сформировать одинаковые образы ошибок. Для сравения двух образов следует использовать правило сравнения образов классов.

Два образа класса формируют разные образы ошибок, если:

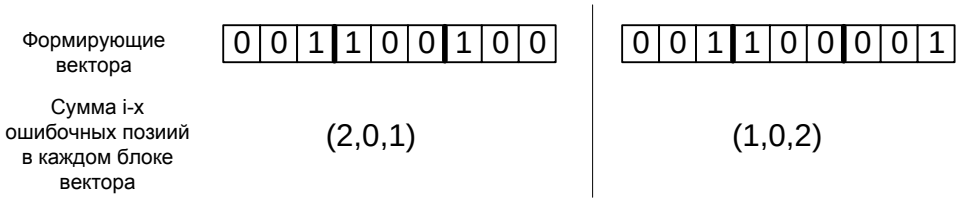
1) количество ошибочных символов в каждом блоке первого образа не совпадает с количеством ошибочных символов в каждом блоке второго образа без учета порядка следования блоков. На рис. 7а показано, что если формирующие вектора определяют один и тот же образ, то сумма ошибочных символов в их блоках совпадает;

2) суммарное количество единиц, стоящих на i-й позиции каждого блока первого образа класса не совпадает с суммарным количеством единиц, стоящих на j-й позиции второго образа класса, $i=\overline{1,t}$, $j=\overline{1,t}$. На рис. 7б показано, что у двух одинаковых образов сумма ошибочных символов у их формирующих векторов по каждой позиции одинакова.

Представление образа класса не как таблицы, а как строки, более удобно для дальнейшей его обработки на ЭВМ.



а)



б)

Рис. 7. Образы классов: *а* – совпадающие по строкам;
б – совпадающие по столбцам

Если сравнение двух образов классов показало, что они формируют разные образы ошибок, то это означает, что сумма их ошибочных позиций по строкам и по столбцам соответственно разная. Однако существуют образы сумма ошибочных символов по строкам и столбцам которых одинакова, но они не являются одинаковыми; такие образы являются нетипичными (рис. 8).

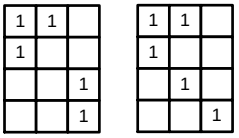


Рис. 8. Нетипичные образы (t=5)

Различить нетипичные образы можно применяя следующее правило:

1) переставлять строки образов согласно уменьшению общего числа ошибочных символов в них;

2) переставлять столбцы образов так, чтобы общее число ошибочных символов в них попарно совпадало;

3) циклически сдвигать строки одного образа, пока его первая строка не совпадет с первой строкой другого образа;

4) если два разных образа представляют собой одну и ту же ошибку, то строки образов совпадут без учета порядка их следования; если же строки образов не совпадут – то они формируют разные ошибки.

Метод формирования библиотеки образов ошибок использует эти правила и требует выполнения следующих этапов:

1) получить все образующие вектора для кратности ошибки t;

2) получить все формирующие вектора для кратности t;

3) распределить формирующие вектора по группам и классам;

4) определить среди классов типичные ошибки и из них оставить только один класс;

5) оставшиеся образы классов формируют все возможные образы пакетных/модульных ошибок.

Алгоритм формирования библиотеки образов ошибок для кратности *t* приведен на рис. 9.

Задачей блока 1 является определение кратности ошибки, для которой определяются образы ошибок. Блок 2 предназначен для генерации образующих векторов. В блоке 3 определяется набор формирующих векторов и производится их распределения по группам и классам внутри группы. В блоке 4 определяется образ класса, а в блоке 5 сравнение образов классов для выявления типичных и нетипичных образов ошибок и, кроме того, определяется множество формирующих векторов, порождающих все образы ошибок кратности *t*.

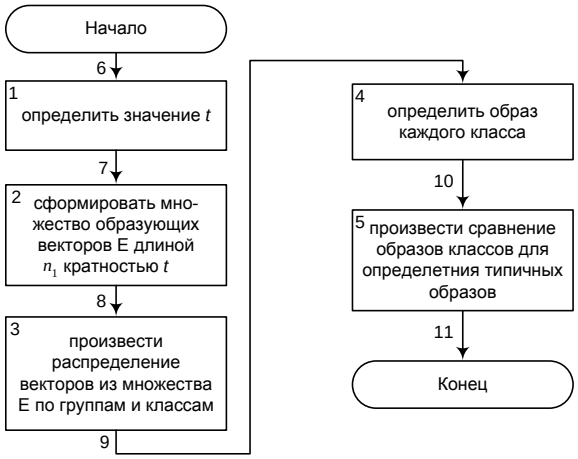


Рис. 9. Алгоритм формирования библиотеки образов ошибок кратности *t*

Выводы

В статье определены понятия образов пакетных и модульных образов ошибок. Показано, что образы зависимых ошибок можно сформировать с помощью соответствующих образующих векторов ошибок. Также показано, что от числа образующих векторов пакетных/модульных ошибок зависит скорость определения всех образов. Предложены методы классификации и поиска образов зависимых ошибок на основе множества образующих векторов.

SEARCH OF TWO-DIMENSIONAL DEPENDENT ERRORS IMAGES

O.G. SMOLYAKOVA, E.G. MAKEICHIK, I.V. KONOPELKO

Abstract

This paper considers a classification of two-dimensional dependent errors images. Determines the vector of dependent errors images. Suggests a method and algorithm for the formation of error packets libraries. Determines the images of module errors.

Литература

1. *Фам Хак Хоан.* Декодирование итеративных кодов на основе коррекции и идентификации ошибок, исправления стираний. Диссертация на соискание ученой степени канд. техн. наук
2. *Конопелько В. К, Фам Хак Хоан.* // Докл. БГУИР. 2007. № 1. 55-60.
3. *Фам Хак Хоан, О.Г. Смолякова.* // Докл. БГУИР. 2008. № 1. 70-75.

УДК 621.391

ПОКАЗАТЕЛИ УСТОЙЧИВОСТИ ЭЛЕМЕНТОВ ИНФРАСТРУКТУРЫ ОТКРЫТЫХ КЛЮЧЕЙ К СЕТЕВЫМ АТАКАМ

В.В. КОЗЛОВСКИЙ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки 6, Минск 220013, Беларусь

Поступила в редакцию 16 октября 2009

Рассматриваются показатели устойчивости элементов инфраструктуры открытых ключей к сетевым атакам.

Ключевые слова: инфраструктура открытых ключей, показатели устойчивости, сетевые атаки.

Введение

В современных системах телекоммуникации для обеспечения информационной безопасности электронных документов и обмена транзакциями применяется технология на основе инфраструктуры открытых ключей (ИОК). Элементы ИОК, включающие в свой состав комплексы программных и аппаратных средств функционирующих в сетевом окружении в соответствии с установленными политиками и процедурами, так же подвергаются различным атакам, в частности – сетевым.

Методы сетевых атак

Анализ существующих классификаций методов и алгоритмов сетевых атак позволяет выделить следующие методы их проведения:

- подмена доверенного объекта ИОК;
- внедрение в ИОК ложного объекта за счет навязывания ложного маршрута;
- отказ в обслуживании за счет создания аппаратного/программного сбоя, уничтожения или изменения информации управления, использования ресурсов.
- передача управления враждебному коду, внедренному в программное обеспечение элемента ИОК (прикладное или системное) [1];

Оценка устойчивости элементов ИОК

Для оценки устойчивости элементов ИОК к сетевым атакам необходимо построить модель системы анализа устойчивости (САУ), описывающую совокупность воздействия на ИОК во время проведения исследований. В модели САУ для ИОК определяем следующие критерии устойчивости:

P(T) – показатель устойчивости элемента ИОК;

H(T) – показатель эффективности конфигурации средств обеспечения устойчивости элемента ИОК;

Метрики для вычисления количественных значений показателей устойчивости:

1) значение показателя устойчивости ИОК при воздействии сетевых атак вычисляется следующим образом

$$P(T) = 1 - D(T) / K, \quad (1)$$

где $D(T)$, K – положительные действительные числа;

$D(T)$ – количество экспериментов, в которых в течение времени T не была восстановлена устойчивость ИОК, нарушенная в результате сетевой атаки;

K – общее количество экспериментов, в ходе которых сетевые атаки приводили к нарушению устойчивости ИОК;

2) значение показателя эффективности конфигурации средств обеспечения устойчивости ИОК вычисляется следующим образом

$$H(T) = 1 - \sum_{i \in V} p_i(t), \qquad t \le T, \tag{2}$$

где T – максимально допустимое время восстановления, измеренное на последовательности интервалов наблюдения;

V – множество невозвратных состояний, т.е. эксперименты, в которых не была восстановлена устойчивость;

$p_i(t)$ – статистическая оценка показателей устойчивости.

Для определения меры устойчивости элемента ИОК к воздействию сетевых атак дополняем существующие критерии оценки устойчивости программных средств по ГОСТ 28195-99 параметром времени T. Таким образом, в формуле (1) для метрики показателя устойчивости элемента ИОК к воздействию сетевых атак время восстановления введено как важный параметр. Допустим, атакующему для осуществления своей цели необходимо в течение времени t нарушить доступность элемента ИОК, для чего он генерирует поток запросов, вызывающий отказ в обслуживании (или сбой). Однако, если за время $T < t$ доступность элемента ИОК восстанавливается, т.е. возвращается в устойчивое состояние, то нарушитель своей цели не достигает [2, 3].

Таким образом, формула (1) определяет показатель P(T) – устойчивости восстановления элемента ИОК при воздействии сетевой атаки, характеризует его способность обеспечивать восстановление работы в заданных режимах и имеет смысл вероятности восстановления устойчивости за время наблюдения $T_н$.

Для определения показателя H(T2) – эффективности конфигурации средств обеспечения устойчивости, – по формуле (2) необходимо наличие большой статистики по показателю устойчивости восстановления. В то же время об эффективности конфигурации средств обеспечения устойчивости ИОК можно судить по показателю эффективности восстановления элемента ИОК при воздействии сетевых атак по отношению к параметру среднее время восстановления T2.

Под нарушением устойчивости понимается временная приостановка выполнения запроса или отказ в выполнении запроса. Чтобы зафиксировать нарушение устойчивости необходимо знать параметр среднее время обработки запроса T1, который либо задается в программной документации на элемент ИОК или вычисляется по формуле

$$T1 = \frac{1}{m} \sum_{j=1}^{m} T_j , \tag{3}$$

где T_j, m – действительные положительные числа;

T_j – время обработки j-го запроса;

m – количество экспериментов меньшее N, т.е. количество запросов в потоке, в которых запросы обслуживались без нарушений;

N – общее количество экспериментов, т.е. запросов в потоке, подаваемых с высокой интенсивностью на исследуемый элемент ИОК.

Зная параметр среднего времени обработки запроса T1 можно вычислить следующие параметры:

K – количество экспериментов, которые завершились с нарушением устойчивости, т.е. когда время ответа на запрос превышает среднее время обработки T1;

T2 – среднее время восстановления на последовательности в N экспериментов.

Среднее время восстановления вычисляется по формуле

$$T2 = \frac{1}{n} \sum_{i=1}^{n} T_i , \tag{4}$$

где T_i, n – действительные положительные числа;

T_i – время восстановления после i-го нарушения устойчивости;

n – количество экспериментов, которые завершились с восстановлением устойчивости.

Тогда метрика определения показателя H(T2) – эффективности средств обеспечения устойчивости, – зависит от параметра среднего времени восстановления T2 и описывается следующей формулой

$$H(T2) = \frac{B(T2)}{K - D(T)}, \quad (5)$$

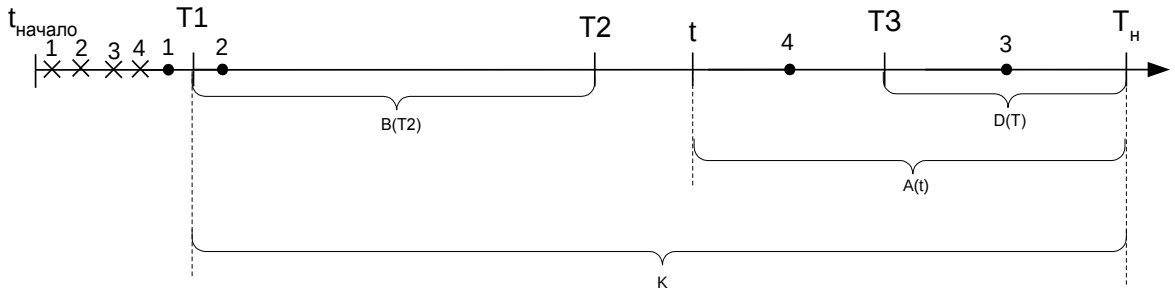
где $B(T2)$, K, $D(T)$ – действительные положительные числа;

$B(T2)$ – количество экспериментов, в которых восстановление устойчивости происходило за среднее время восстановления T2;

K – количество экспериментов, которые завершились с нарушением устойчивости;

$D(T)$ – количество экспериментов, в которых воздействие сетевых атак приводило к отказу, т.е. ответ на запрос не пришел или пришел с кодом отказа за время наблюдения $T_н$.

Для облегчения понимания на рисунке приведена временная диаграмма проведения N экспериментов.



Временная диаграмма проведения N экспериментов

Таким образом, показатель H(T2) характеризует способность элемента ИОК за среднее время восстановления после отклонений, вызванных воздействием сетевых атак, восстанавливать устойчивую работу и имеет смысл вероятности восстановления устойчивой работы за среднее время восстановления.

Для определения меры устойчивости элемента ИОК к воздействию сетевых атак необходимо ввести дополнительные показатели оценки:

- R(T) – показатель устойчивого функционирования при воздействии сетевых атак;
- G(T) – показатель безотказности работы;
- M(T) – показатель успешности восстановления;

Метрика определения показателя R(T) – устойчивого функционирования при воздействии сетевых атак, – также зависит от параметра времени и описывается следующей формулой

$$R(T) = 1 - \frac{K - D(T)}{N}, \quad (6)$$

где K, $D(T)$, N – действительные положительные числа;

$K - D(T)$ – количество экспериментов, в которых восстановлена устойчивость за время наблюдения $T_н$;

N – количество экспериментов, т.е. количество запросов в потоке.

Показатель R(T) характеризует способность элемента ИОК обеспечивать устойчивую работу без возникновения отклонений, вызванных воздействием сетевых атак, и имеет смысл вероятности выполнения работы без нарушения.

Метрика определения показателя G(T) – безотказности работы, – также зависит от параметра времени и описывается следующей формулой

$$G(T) = 1 - \frac{D(T)}{N}, \tag{7}$$

где *D(T), N* – действительные положительные числа;

D(T) – количество экспериментов, в которых воздействие удаленных активных атак приводило к отказу;

N – количество экспериментов.

Показатель G(T) характеризует способность элемента ИОК при воздействии сетевых атак обеспечивать выполнение всех запросов за время наблюдения $T_н$ (т.е. обеспечивать продолжения работы без отказов) и имеет смысл вероятности безотказной работы.

Метрика определения показателя M(T) – успешности восстановления, –также зависит от параметра времени и описывается следующей формулой

$$M(T) = \frac{K - A(t)}{K - D(T)}, \tag{8}$$

где *K, A(t), D(T)* – действительные положительные числа;

K - A(t) – количество экспериментов, в которых восстановлена устойчивость за время t;

K - D(T) – количество экспериментов, в которых восстановлена устойчивость за время наблюдения $T_н$;

A(t) – количество экспериментов, в которых нарушения устойчивости не восстановлены за время t;

t – время наблюдения на интервале T2 < t < T3, т.е. большее среднего времени восстановления, но меньшее времени отказа.

Показатель M(T) характеризует способность элемента ИОК при воздействии сетевых атак обеспечивать восстановление времени работы за время большее среднего времени восстановления и имеет смысл вероятности выполнения восстановления за время t.

Перечень показателей устойчивости элементов ИОК к воздействию сетевых атак

Критерий устойчивости	Обозначение	Свойство
Устойчивость восстановления при воздействии сетевых атак	P(T)	Способность элемента ИОК при возникновении отклонений, вызванных воздействием сетевых атак, обеспечивать восстановление своей работы в заданных режимах
Устойчивость функционирования при воздействии сетевых атак	R(T)	Способность элемента ИОК обеспечивать устойчивую работу без возникновения отклонений, вызванных воздействием сетевых атак
Эффективность средств обеспечения устойчивости	H(T2)	Способность элемента ИОК за среднее время восстановления после отклонений, вызванных воздействием сетевых атак, восстанавливать устойчивую работу
Безотказность работы	G(T)	Способность элемента ИОК обеспечивать продолжение работы без отказов после возникновения отклонений, вызванных воздействием сетевых атак
Успешность восстановления	M(T)	Способность элемента ИОК после отклонений, вызванных воздействием сетевых атак, обеспечивать восстановление своей работы в заданных режимах за время большее среднего времени восстановления

Заключение

Проведенные исследования показали необходимость выбора показателей устойчивости, которые поддаются измерению при испытаниях элементов ИОК. При оценке испытуемых элементов ИОК должны быть учтены особенности и ограничения по их функционированию.

INDICATORS OF THE SUSTAINABILITY OF THE ELEMENTS OF PUBLIC KEY INFRASTRUCTURE FOR NETWORK ATTACKS

V.V. KOZLOVSKI

Abstract

Discusses the indicators of the sustainability of the elements of public key infrastructure for network attacks.

Литература

1. *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI, М., 2004.
2. *Громов Ю.Ю., Драчев В.О.* Синтез и анализ живучести сетевых систем. М., 2007.
3. *Хорев П.Б.* Методы и средства защиты информации в компьютерных системах. М., 2005.

УДК 621.391

МЕЖСЕТЕВЫЕ ЭКРАНЫ

Ф.О. МОХАММЕД

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 26 октября 2009

Используемые межсетевым экраном механизмы служат для предотвращения или блокирования нежелательного трафика. Такими механизмами, могут быть: простой пакетный фильтр, который принимает решения в зависимости от содержания заголовка пакета; или анализатор состояния который проверяет, что данный пакет является частью законного потока; или более сложный механизм такой как прокси-сервер который устанавливается между клиентом и внешней сетью.

Ключевые слова: межсетевой экран (МСЭ), пакетный фильтр, контроль состояния, прокси-сервер.

Введение

Межсетевые экраны обеспечивают барьер между сетями и предотвращают или блокируют нежелательный или несанкционированный трафик. Единственного определения для межсетевого экрана не существует. В данной работе будем использовать следующее определение межсетевого экрана. Межсетевой экран – система или группа систем, используемая для управления доступом между доверенными и не доверенными сетями на основе предварительно сконфигурированных правил [1].

Межсетевые экраны могут управлять доступом к сети и от нее. Они могут настраиваться для предотвращения получения доступа к внутренним сетям и услугам несанкционированных пользователей. Они могут также конфигурироваться для предотвращения нежелательного доступа к внешним или несанкционированным сетям и услугам внутренних пользователей. МСЭ обеспечивает также выполнение следующих функций:

Установление подлинности пользователя: межсетевые экраны могут настраиваться для обеспечения установления подлинности пользователя. Это позволяет администраторам сетей управлять доступом определенных пользователей к определенным услугам и ресурсам. Установление подлинности также позволяет администраторам сетей отслеживать определенную деятельность пользователя и попытки получить несанкционированный доступ к защищенным сетям или услугам.

Аудит и регистрация: межсетевые экраны могут обеспечить аудит и регистрацию действий, сохранить и проанализировать эту информацию позднее. Межсетевые экраны тоже могут произвести статистику, основанную на информации, которую они собирают. Эти статистические данные очень полезны администраторами безопасности при принятии решений.

Безопасность: некоторые функции межсетевых экранов позволяют скрыть внутренние или доверенные сети, от внешних или не доверенных сетей. Это помогает в ограждении услуг от нежелательных просмотров. Когда людские и финансовые ресурсы ограничены, межсетевые экраны могут являться центральной точкой управления безопасности.

Наряду с достоинствами межсетевые экраны обладают рядом недостатков:

Транспортные узкие места: в некоторых сетях межсетевые экраны создают транспортное узкое место. Они вынуждают все межсетевые трафики проходить через межсетевой экран, поэтому есть большая вероятность, что сеть станет переполненной.

Единственный пункт отказа: межсетевые экраны могут создать единственный пункт отказа. В большинстве конфигураций, где межсетевые экраны являются единственной связью между сетями, если они недоступны или конфигурируются не правильно, то никакой трафик через них не пройдет.

Повешенная ответственность администратора: межсетевой экран часто добавляет ответственность в управление сетью и делает обслуживание сети более сложным, потому что все межсетевые экраны требуют длительной административной поддержки в виде обновлений программного обеспечения и перенастройки политик безопасности.

Для управления доступом к сети, межсетевые экраны используют один из двух принципов защиты:

1. Все неопределенно разрешенное, запрещено.
2. Все неопределенно запрещённое, разрешено.

У каждого принципа есть сторонники, но первый принцип чаще всего рекомендуемый. Он базируется на предпосылке, что если определенные правила разрешения отсутствуют, то доступ запрещен.

Второй принцип имеет противоположную логику. Доступ запрещается, если для этого сформированы определенные правила. Если правил нет, то доступ полностью открыт.

Типы межсетевых экранов

Для построения межсетевого экрана используется определенный метод проверки пакета. В каждом методе используется информация от различных уровней модели взаимосвязи открытых систем. Известные три типа межсетевых экранов:

1. Пакетные фильтры (Packet filtering),
2. МСЭ с контролем состояния (Stateful packet inspection),
3. Прикладной шлюз/прокси (Application gateways/proxies).

Гибридные методы проверки пакетов комбинируют два или более из них для обеспечения повышенных возможностей и безопасности.

Пакетные фильтры

Пакетные фильтры (рис. 1) – самый простой метод проверки пакета. Процесс фильтрования пакета заключается в исследовании информации содержащейся в заголовке и сравнении ее с предварительно сконфигурированной группой правил или фильтрами. Каждый пакет может, исследоваться индивидуально без отношения к другим пакетам, несмотря на то, что они могут являться частью одного трафика [2].

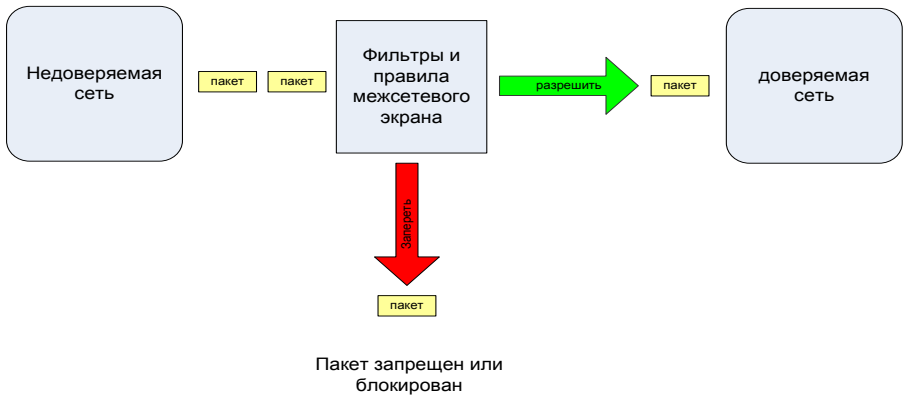


Рис. 1. Межсетевой экран – пакетный фильтр

Пакетные фильтры часто называют межсетевыми экранами уровня сети, потому что процесс фильтрования происходит на сетевом уровне (третий уровень) или транспортным уровне (четвертый уровень) модели OSI. Рис. 2 показывает отношение между пакетным фильтром и моделью OSI [3, 4].

Рис. 2. Пакетный фильтр и уровни OSI

Правила пакетной фильтрации или фильтры могут быть сконфигурированы на основе разрешения или запрета. Конфигурация правил фильтрования пакета основывается на одном или более следующих параметров:

- IP адрес источника,
- IP адрес назначения,
- Тип протокола,
- Порт источника,
- Порт назначения.

Достоинства

Пакетные фильтры функционируют быстрее, чем другие типы МСЭ, так как фильтруют пакеты на более низких уровнях модели OSI. Если они настроены правильно, то пакетные фильтры оказывают очень малое влияние на работу сети.

Пакетные фильтры могут быть установлены прозрачным образом. Они не требуют никакой дополнительной конфигурации для клиентов.

Пакетные фильтры межсетевых экранов дешевле, чем другие методы проверки пакета.

Пакетные фильтры являются независимыми от приложения, так как их решения основаны на информации, содержащейся в заголовке пакета, а не на информации, которая имеет отношение к определенному приложению.

Недостатки

Если порт был открыт МСЭ, то он открыт для всех проходящих трафиков через этот порт.

Определение правил и фильтров в этом методе является сложной задачей. У администратора сети должно быть хорошее понимание услуг и протоколов для выполнения требования безопасности.

Проверка точности выполнения правил на пакетном фильтре является очень трудной задачей. Даже если правила кажутся простыми и явными, проверка их правильности путём тестирования отнимает много времени и не всегда даёт правильный результат.

МСЭ с контролем состояния

МСЭ с контролем состояния исследует информацию заголовков пакетов от сетевого уровня до прикладного уровня модели OSI и проверяет, что данный пакет является частью законного потока и используются допустимые протоколы. рис. 3 показывает отношению между МСЭ с контролем состояния и моделью OSI.

Рис. 3. МСЭ с контролем состояния и уровни OSI

МСЭ с контролем состояния работает следующим образом (рис. 4). Заголовки TCP пакета проверяются для определения, является ли пакет частью уже существующего и действующего потока передаваемых данных. Межсетевой экран имеет активную таблицу всех текущих сеансов и сравнивает входящие пакеты с её данными в процессе контроля доступа. Если в таблице отсутствует соответствующий вход соединения, МСЭ проверяет пакет с использованием установленного набора правил, аналогичного фильтру пакетов. Если проверка по правилам фильтрации прошла успешно и передача пакета разрешается, МСЭ создает или обновляет свою таблицу соединений. Внесенный вход соединения будет использоваться для проверки последующих пакетов вместо правил фильтрации. В качестве параметров проверки состояния используются:

- IP адрес источника,
- IP адрес назначения,
- Тип Протокола,
- Порт источника,
- Порт назначения,
- Состояние связи.

Состояние связи определяется из информации собранной на основе анализа предыдущих пакетов. Это - существенный фактор в принятии решения при новых попытках открыть соединение. МСЭ с контролем состояния сравнивает пакеты с правилами или фильтрами и затем по динамической таблице состояния, проверяет, что все пакеты - часть действительной и установленной связи.

Этот метод защищает сети от атаки лучше, чем методы экранирования пакетов, потому что он имеет возможность анализа состояния связи.

Достоинства

МСЭ с контролем состояния, как и пакетные фильтры, оказывают очень небольшое влияние на работу сети, они реализуется прозрачно, и являются независимыми от приложений.

МСЭ с контролем состояния более безопасны, чем пакетные фильтры. Так как производят более глубокий анализ заголовка пакета для определения состояния связи между конечными точками.

Анализируя информацию заголовка пакета, МСЭ с контролем состояния может проверить, что протоколы прикладного уровня работают правильно.

У МСЭ с контролем состояния обычно есть некоторые возможности по регистрации. Регистрация может помочь идентифицировать и отследить различные типы трафиков, проходящие через межсетевой экран.

Недостатки

Как и пакетные фильтры, МСЭ с контролем состояния не нарушает модель клиент/сервер и разрешает прямое соединение между этими двумя конечными точками.

Правила и фильтры этого метода могут быть достаточно сложными и трудными для восприятия.

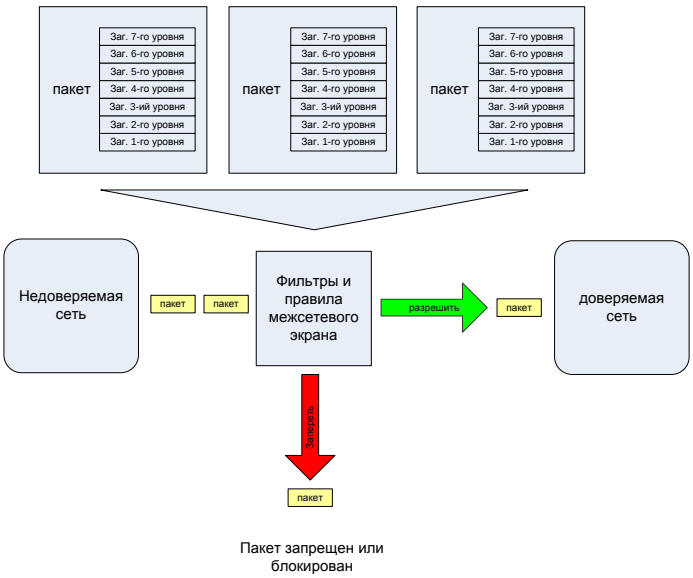


Рис. 4. МСЭ с контролем состояния

Прокси-серверы

Прокси-серверы обычно реализуются на безопасной системе хоста, формируемой с двумя интерфейсами сети. Прокси-серверы являются посредниками между этими двумя конечными точками. Этот метод проверки пакета нарушает модель клиент-сервер и осуществляет вместо этой модели две связи: первая связь от источника к прокси-серверу и вторая от прокси-сервера к назначению. Каждая конечная точка может общаться с другими точками только проходя прокси-сервер.

Этот тип межсетевого экрана работает на прикладном уровне модели OSI. Для соединения конечных точек источников с точками назначений, прокси-сервер должен быть реализован в каждом протоколе прикладного уровня. Рис. 5 показывает отношения между прокси-серверами и моделью OSI.

Прикладной	Прокси-серверы
Представит.	
Сеансовый	
Транспортный	
Сетевой	
Канальный	
Физический	

Рис. 5. Прокси-серверы и уровни OSI

Прокси-сервер работает следующим образом (рис. 6). Когда клиент делает запрос из недоверяемой сети, связь устанавливается с прокси-сервером. Прокси-сервер определяет, действителен ли запрос (сравнивая его с правилами или фильтрами) и затем посылает новый запрос от себя к назначению. При использовании этого метода прямая связь от доверяемой сети до недоверяемой сети, никогда не осуществляется, и запрос представляется пришедшим от прокси-сервера.

Ответ отсылается назад к прокси-серверу и затем пересылается клиенту. Нарушая модель клиент-сервер, этот тип межсетевого экрана может эффективно скрыть доверяемую сеть от недоверяемой сети.

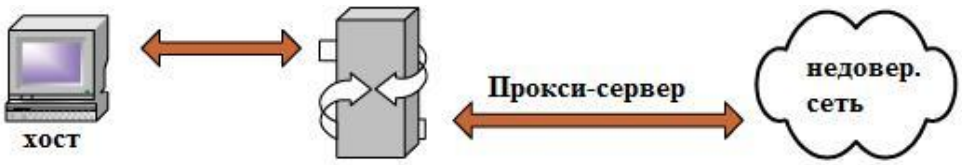


Рис. 6. Прокси-сервер межсетевой экран

В отличие от пакетного фильтра и МСЭ с контролем состояния, прокси-сервер может видеть все аспекты прикладного уровня, и таким образом может исследовать более определенную информацию. Например, он может найти различие между частью электронной почты содержащей текст и содержащей графическое изображение, или различие между веб-страницами (web page) с использованием языка Java и веб-страницами без Явы. С точки зрения безопасности прокси-серверы выше других типов экранирования пакета, Но этот метод не всегда является самым практичным для использования.

Достоинства

Прокси-сервер не позволяет прямую связь между конечными точками. Он нарушает модель клиент-сервер. В этом отношении, этот метод действительно разделяет внутренние и внешние сети.

Прокси-сервер не реализует прямой маршрут между сетями. Так как никакая маршрутизация не делается, этот метод обеспечивает трансляцию сетевых адресов (Network Address Translation (NAT)).

Прокси-серверы позволяют администратору сети иметь больше контроля над трафиком, проходящим через межсетевой экран. Они могут разрешить или запретить определенные приложения или определенные особенности приложений.

У прокси-серверов есть лучшие способности фильтрования. Так как у них есть способность исследовать информационную часть пакета, они способны к принятию решений, основанному на содержании.

Недостатки

На прокси-серверах весь исходящий и входящий трафик проверяется на прикладном уровне, поэтому они медленнее, чем пакетные фильтры и МСЭ с контролем состояния, которые проверяют трафик на сетевом уровне. В этом методе все трафики должны пройти через все уровни модели OSI, в результате инспекционный процесс требует много времени обработки. Это может привести и тому, что МСЭ может стать узким местом в сети.

Другой недостаток прокси-сервера состоит в том, что каждый протокол требует своей собственной привязки к прокси-серверу. Если такой привязки не существует, то соответствующий протокол не может проходить через межсетевой экран. Кроме того, так как для каждого протокола требуется свой собственный прокси-сервер, поддержка новых протоколов может стать трудным делом.

Прокси-серверы требуют дополнительных конфигураций клиента. Клиентам на сети может потребоваться специализированное программное обеспечение, чтобы быть в состоянии соединиться с прокси-сервером. Это может оказать сильное влияние на большие сети с многочисленными клиентами.

Масштабируемость может быть проблемой с прокси-серверами, когда они установлены в больших сетях. Потому что, если число клиентов или число прокси-серверов расположенных на одном хосте увеличивается, то работа ухудшается.

Прокси-серверы, установленные на операционных системах общего назначения, уязвимы для лазеек безопасности основной системы. Если основная система не безопасна, то межсетевой экран не безопасен.

Заключение

МСЭ представляет собой эффективное средство, реализующее контроль за информацией, поступающей в локальную сеть и/или выходящей из нее, посредством анализа по совокупности критериев и правил принятия решения о ее распространении в локальной сети.

FIREWALLS

F. O. MOHAMMED

Abstract

The mechanisms that used by the firewall to allow or block traffic can be simple packet filters, which make decisions based on the contents of the packet header, or stateful packet inspection which checks the state of all current connections, or more complex application proxies, which stand between the client and the outside world, acting as a middleman for some network services.

Литература

1. *David Hucaby*. Cisco ASA, PIX, and FWSM Firewall Handbook // Cisco press, Second Edition. 2008.
2. *Vitaly Osipov, Mike Sweenety,Woody Weaver, Charles E. Riley, Umer Khan*. // Cisco Security Specialist's guide to PIX Firewall. 2002.
3. *Terry Ogletree*. // Practical Firewalls. 2000.
4. *Wes Noonan, Ido Dubrawsky*. // Firewall Fundamentals. 2006.

УДК 519.711.4 (075.8)

АЛГЕБРАИЧЕСКИЕ БАЗИСНЫЕ МЕТОДЫ ФОРМИРОВАНИЯ И ОБРАБОТКИ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Н.В. ЧЕСАЛИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 26 октября 2009

Сделан краткий обзор по проблемам генерации и обработки периодических кодовых последовательностей. Предложен новый подход к формированию последовательностей и исследованию их свойств. Методы связаны с построением нормальных базисов в полях Галуа.

Ключевые слова: кодовая последовательность, поле Галуа, нормальный базис, регистр сдвига.

Введение

Периодические кодовые последовательности в настоящее время имеют большое научное и прикладное значение. Они используются, прежде всего, в радиолокационных и навигационных системах, системах мобильной связи и криптографии.

Изучению свойств различных классов периодических последовательностей посвящены, например, монографии [1, 2], в которых, в частности, была приведена классификация периодических последовательностей по некоторым выделенным свойствам. Однако до сих пор остаются нерешенными многие проблемы данной теории, которые сформулированы в виде гипотез [3]. Это, прежде всего, гипотеза о существовании бесконечного числа примитивных трехчленов, о циклических разностных множествах Адамара, о совпадении класса двоичных M-последовательностей с классом периодических последовательностей сдвигового регистра линейной сложности n, обладающих идеальной автокорреляционной функцией и многие другие.

В ряде ситуаций, возникающих в работе компьютеров, в криптографии и многочисленных других областях появляется необходимость использования случайных последовательностей из нулей и единиц. Здесь под случайностью понимается непредсказуемость последовательности. Более точно, требуются последовательности, которые бы выглядели как случайные, но при более глубоком анализе можно было бы найти определенную регулярность. Первоначально были выделены три характеристических свойства двоичных последовательностей над полем Галуа $GF(2)$, характеризующих их случайность. Это сбалансированность, определенное соотношение для числа идущих подряд 1 и 0 и свойство автокорреляции. Затем эти свойства были обобщены на случай последовательностей над произвольным полем Галуа $GF(q)$. Всестороннее изучение M– последовательностей привело к открытию ряда новых свойств, которые продолжили аксиоматику случайных последовательностей.

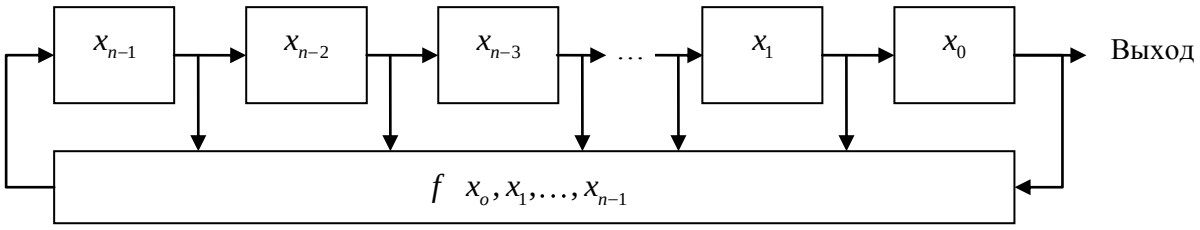


Рис. 1. Блок-схема n-уровневого регистра сдвига с обратной связью конфигурации Фибоначчи

Одним из классических методов задания периодических последовательностей является рекурсия. Физическая реализация процесса построения периодических последовательностей осуществляется с помощью n-уровневого регистра сдвига на триггерах [4]. В настоящее время используются два основных типа регистров сдвига с обратной связью: либо с конфигурацией Фибоначчи, либо с конфигурацией Галуа. На рис. 1 рассмотрена блоковая диаграмма первого процесса. Таким образом, задается линейный регистр сдвига с обратной связью (LFSR), если булева функция $f\ x_0, x_1, ..., x_{n-1}$ является линейным отображением из $0,1^{\ n}$ в $0,1$, и задается нелинейный регистр сдвига с обратной связью (NLFSR) в противном случае. Блоковая диаграмма второго процесса представлена на рис. 2.

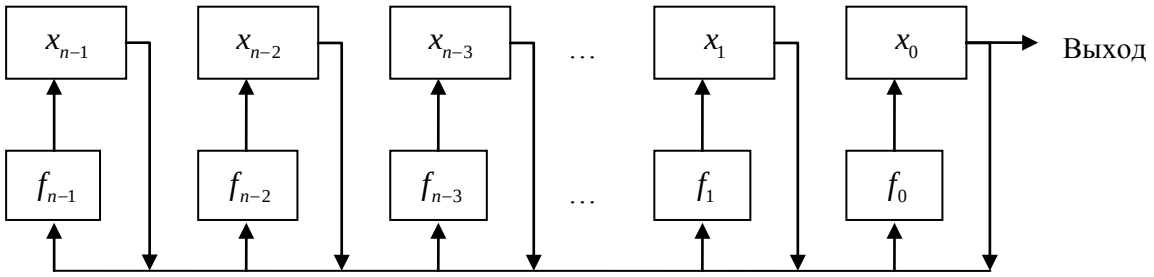


Рис. 2. Блок-схема n-уровневого регистра сдвига с обратной связью конфигурации Галуа

Как видно из приведенных блок-схем конфигурация Галуа концептуально значительно сложнее конфигурации Фибоначчи. В работе [5] было установлено, что для любого NLFSR конфигурации Фибоначчи существует класс соответствующих эквивалентных регистров сдвига конфигурации Галуа. Вопрос обратного соответствия остается открытым, как и построение систематических алгоритмов для синтеза NLFSR, обеспечивающих заданные длинные периоды генерируемых последовательностей. Следует отметить, что для генерации последовательностей также используются конфигурации регистров с обратной связью более общего вида (не обязательно регистры сдвига) [6]. Пример такой конфигурации схематически изображен на рис. 3.

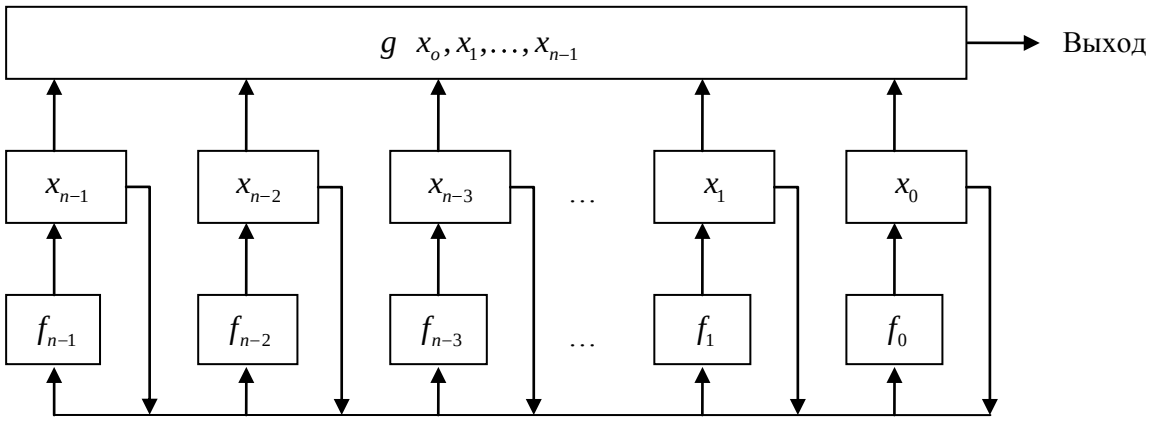


Рис. 3. Блок-схема n-уровневого регистра с обратной связью общей конфигурации

На последних двух блок-схемах g и f_i – булевы функции, действующие из $0,1^n$ в $0,1$, $0 \le i \le n-1$.

Одной из важнейших характеристик генерируемых последовательностей является их линейная сложность (Linear Complexity). Она характеризует степень сложности процесса генерации и криптографические свойства последовательности.

В настоящей работе, используя анализ различных методов формирования кодовых последовательностей, разрабатываются некоторые новые подходы к формированию и изучению важнейших свойств кодовых последовательностей. Основу здесь составляет представление периодических последовательностей элементами подходящего поля Галуа в нормальном базисе и использование базисов Гребнера для линеаризации систем булевых функций и исследования линейной сложности.

Периодические последовательности и нормальные базисы

В поле $GF\ q^n$, рассматриваемом как n-мерное векторное пространство над полем $GF\ q$, где q – степень некоторого простого числа, всегда можно ввести базис вида

$$N = \alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}} , \qquad 0 \ne \alpha \in GF\ q^n .$$

Данный базис называется нормальным. Далее, через $T = t_{ij}$ обозначим квадратную матрицу $n \times n$, определенную равенствами

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \le i \le n-1, \qquad t_{ij} \in GF\ q , \qquad \alpha_i = \alpha^{q^i}.$$

Число ненулевых элементов матрицы T называется сложностью нормального базиса N и обозначается через c_N. Имеет место оценка $c_N \ge 2n-1$. если $c_N = 2n-1$, то базис N называется оптимальным нормальным базисом. Заметим, что для $a \in GF\ q^n$, $a \ne 0$, $aN = a\alpha_0, a\alpha_1, ..., a\alpha_{n-1}$ – также нормальный базис; базисы N и aN называются эквивалентными. Как известно, нормальный базис N эквивалентен своему двойственному базису (совпадает со своим двойственным базисом) тогда и только тогда, когда матрица T – симметрическая (и след $Tr_n\ \alpha^2 = 1$, где α – элемент, порождающий базис N). Оптимальные нормальные базисы были открыты Mullin, Onyszchuk, Vanstone и Wilson [7]. Имеют место следующие результаты.

Теорема 1. (Тип 1 оптимальных нормальных базисов) Предположим, что число $n+1$ – простое и число q является примитивным элементом в $\mathbf{Z}_{n+1}$. Тогда n корней степени $n+1$ из единицы (кроме 1) образуют оптимальный нормальный базис в $GF\ q^n$ над полем $GF\ q$.

Теорема 2. (Тип 2 оптимальных нормальных базисов) Пусть число $2n+1$ – простое и либо число 2 является примитивным элементом в $\mathbf{Z}_{2n+1}$, либо число 2 порождает квадратичные вычеты в $\mathbf{Z}_{2n+1}$ и $2n+1 \equiv 3 \bmod 4$. Тогда $\alpha = \gamma + \gamma^{-1}$ порождает оптимальный нормальный базис в $GF\ 2^n$ над полем $GF\ 2$, где γ – примитивный корень степени $2n+1$ из 1.

В 1992 году Gao и Lenstra доказали, что каждый оптимальный нормальный базис в $GF\ q^n$ над полем $GF\ q$ эквивалентен одному из базисов теорем 1 либо 2. Кроме того, оптимальный нормальный базис N является самодвойственным тогда и только тогда, когда N – оптимальный нормальный базис первого типа и $q = n = 2$ либо N – оптимальный нормальный базис второго типа [8].

Для аналитического описания и исследования свойств периодических функций будем использовать функцию следа $Tr_n\ x = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}}, x \in GF\ p^n$, которая является линейным оператором из $GF\ p^n$ в $GF\ p$, p – простое число.

Для получения различных представлений периодических последовательностей с использованием функции следа оказалось эффективным введение на множестве $\mathbf{Z}_T$ специального отношения эквивалентности, которое разбивает это множество на циклотомические классы C_s, где

$$C_s = s, sq, sq^2, \ldots, sq^{n_s-1}, \qquad sq^{n_s} \equiv s \bmod T,$$

n_s – наименьшее такое натуральное число, T делит $q^n - 1$ и q – степень простого числа. В качестве индекса s циклотомического класса C_s удобно выбирать наименьшее положительное число из данного класса, называемое лидером циклотомического класса. Множество всех лидеров циклотомических классов по модулю T обозначим через L.

Пусть S_T – множество всех T – периодических последовательностей над полем $GF\ p$ и F – множество всех функций из $GF\ p^n$ в $GF\ p$. След-представление периодических последовательностей выражает следующая теорема [2].

Теорема 3. Для любой последовательности $u = u_0, u_1, \ldots, u_{T-1} \in S_T$, T делит $p^n - 1$, существует функция $f\ x \in F$ такая, что

$$f\ x = \sum_{i=1}^{r} Tr_{n_i}\ a_i x^{s_i}, \qquad a_i \in GF\ p^{n_i}, \qquad u_i = f\ \alpha^i,$$

где α – примитивный элемент поля $GF\ p^n$, s_i – лидер циклотомического класса по модулю $p^{n_i} - 1$, n_i – размер циклотомического класса, содержащего s_i, n_i делит n.

Функцию $f\ x$ называют след-представлением r – членной последовательности u. В частности, при $r = 1$ получаем представление M-последовательностей. Однако, следует заметить, что для применения записанной выше формулы на практике требуется описание всех промежуточных полей Галуа и полное описание соответствующих циклотомических классов, что при больших значениях составного числа n является весьма сложной вычислительной задачей.

В данной работе предлагается следующий способ формирования и последующего изучения свойств периодических последовательностей. Для простоты изложения будем рассматривать T – периодические последовательности над полем $GF\ 2$.

Рассмотрим в поле $GF\ 2^T$ нормальный оптимальный базис N, порожденный элементом $\alpha \in GF\ 2^T$. Тогда для любого элемента $u \in GF\ 2^T$ разложение по базису N имеет вид

$$u = u_0\alpha_0 + u_1\alpha_1 + \ldots + u_{T-1}\alpha_{T-1}, \qquad Tr_T\ u = u_0 + u_1 + \ldots + u_{T-1}.$$

Согласно [8] можно выбрать другой нормальный оптимальный базис $M = \beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{T-1}}$, $0 \neq \beta \in GF\ 2^T$, являющийся двойственным к N. Как и ранее, вводя обозначение $\beta_i = \beta^{2^i}$, элемент u может быть записан в виде $u = \sum_{i=0}^{T-1} Tr_T\ u\beta_i\ \alpha_i = \sum_{i=0}^{T-1} Tr_T\ u\alpha_i\ \beta_i$.

Каждую последовательность из множества S_T можно рассматривать как последовательность коэффициентов разложения по нормальному базису. Следовательно, таким образом, строится взаимно-однозначное соответствие множества S_T и поля $GF\ 2^T$. С другой стороны, элементы поля $GF\ 2^T$ допускают стандартную запись с помощью некоторого

примитивного многочлена $p\ x$ в виде многочленов степени не выше $T-1$ с коэффициентами из $GF\ 2$. Обозначая через $\tilde{S}_{T,p\ x}$ множество всевозможных последовательностей, образованных коэффициентами описанных выше многочленов, получаем отображение $G: S_T \to \tilde{S}_{T,p\ x}$, которое устанавливает аналитическую связь между основными параметрами данной модели и инвариантные свойства которого позволяют проводить соответствующую классификацию T-периодических последовательностей. Особый интерес представляют спектральные последовательности, полученные применением дискретного преобразования Фурье и их инвариантные свойства, такие как, например, циклотомическая инвариантность [9], постоянство числа ненулевых компонент спектральных последовательностей, исходные последовательности которых имеют фиксированную линейную сложность и др.

Кроме того, имеет место цепочка включений

$$GF\ 2\ \subset GF\ 2^T\ \subset GF\ 2^{2^n-1}$$

при условии, что $2^n-1=Tm$. Это позволяет рассматривать поле $GF\ 2^{2^n-1}$ как m-мерное векторное пространство над полем $GF\ 2^T$ и моделировать двумерные массивы двоичных последовательностей (типа GMW последовательностей и их обобщений).

Как известно, периоды последовательностей, генерируемых нелинейными регистрами, удовлетворяют оценке $T \le 2^n$. Следовательно, минимальным расширением поля $GF\ 2$, необходимым для полного описания генерируемых последовательностей по аналогичной схеме, является поле $GF\ 2^{2^n}$. Задача точного вычисления либо оценки сверху линейной сложности последовательностей в нелинейном случае решается с помощью базисов Гребнера [10] идеалов полиномиальных колец, порожденных нелинейными функциями f, g и f_i, $0 \le i \le n-1$.

Заключение

Данная работа содержит как краткий обзор по проблемам генерации и обработки периодических кодовых последовательностей, так и новый концептуальный подход к формированию и исследованию свойств периодических последовательностей, основанный, прежде всего, на использовании специальных алгебраических базисов в полях Галуа и полиномиальных кольцах. Статистический материал, полученный на основе численного компьютерного анализа примеров по описанной схеме для различных значений числа n занимает достаточно большой объем и ему будет посвящена отдельная публикация.

ALGEBRAIC BASE METHODS OF GENERATION AND PROCESSING OF CODE SEQUENCES

N.V. CHESALIN

Abstract

Different problems of periodic code sequences in finite fields are considered. A new mode of investigation such sequences is developed. In this research normal bases of Galois fields are applied.

Литература

1. *Golomb S.W.* // Shift Register Sequences. 1982. P. 247.
2. *Golomb S.W., Gong G.* // Signal Design for Good Correlation – Wireless Communication, Cryptography, and Radar. 2005. P. 438.
3. *Golomb S.W.* // Solved and Unsolved Problems Springer-Verlag Berlin Heidelberg. 2007. P.1-8.
4. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М., 1976.
5. *Dubrova E.* // An Equivalence Preserving Transformation from the Fiibonacci to the Galois NLFSRs.2008. P. 1-14.
6. *Chan A.H., Goresky M., Klapper A.* // On the Linear Complexity of Feedback Registers. 1990. Vol. 36, №3. P.640-644.
7. *Mullin R.C., Onyszchuk I.M., Vanstone S.A., Wilson R.M.* // Optimal Normal Bases of $GF(p^n)$ 1989. P.149-161.
8. *Liao Q.Y., Sun Q.* // Normal Bases and Their Dual-Bases over Finite Fields. Vol. 22, № 3. 2006. P.845-848.
9. *Липницкий В.А., Чесалин Н.В.* // 10 БМК. М., 2008.
10. *Кокс Д., Литл Дж., О`Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. М., 2000.

КРАТКИЕ СООБЩЕНИЯ

УДК 621.315.5

ИНТЕГРАЛЬНЫЕ ПАНЕЛИ ЭЛЕКТРОМАГНИТНО-АКУСТИЧЕСКОЙ ЗАЩИТЫ НА ОСНОВЕ ВСПЕНЕННЫХ МАТЕРИАЛОВ

Х.М. АЛЬЛЯБАД, С.Н. ПЕТРОВ, А.М. ПРУДНИК

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 3 ноября 2009

Приведены результаты исследования электромагнитных и акустических характеристик многослойных материалов на вспененной основе для создания панелей интегральной защиты. Показана возможность создания многослойных панелей с величиной ослабления электромагнитных волн более 30 дБ и индексом изоляции воздушного шума 35 дБ.

Ключевые слова: электромагнитное излучение, акустическая волна, защитные материалы, эффективность экранирования, звукоизоляция.

Введение

Одним из направлений разработки современных систем пассивной защиты информации является разработка материалов и конструкций, обеспечивающих подавление как электромагнитных, так и акустических сигналов, позволяющих таким образом снизить риск перехвата информации при ее передаче и обработке, и обеспечить многофакторную защиту объектов. Также такие материалы электромагнитно-акустической защиты могут применяться для обеспечения электромагнитной совместимости радиоэлектронной аппаратуры и для снижения радиолокационной заметности объектов военной техники. Кроме того, они могут быть применены для создания средств защиты биологических объектов от воздействия электромагнитного излучения (ЭМИ).

Комбинированные панели электромагнитно-акустической защиты предназначены для защиты от утечки информации по техническим (электромагнитным и акустическим) каналам. Защита информации с помощью комбинированных панелей электромагнитно-акустической защиты заключается в установке панелей в строительные элементы конструкций зданий (стены, перекрытия) и дверные тамбуры, что предотвращает возможность перехвата информационных электромагнитных полей и съема акустической информации с помощью технических устройств.

Радио- и звукопоглощающие материалы могут быть использованы как при строительстве и отделке помещений, так и для создания модульных разборных конструкций. При этом массогабаритные характеристики разборных конструкций имеют существенное значение. Основным принципом экранирования как электромагнитных, так и акустических сигналов является перенаправление энергии колебаний за счет отражения от поверхностей с геометрическими неоднородностями, а также на поглощении волн внутри материалов. При этом для увеличения эффективности экранирования предпочтение отдается многослойным структурам из материалов с различными электрическими, магнитными и звукопоглощающими свойствами, что позволяет значительно снизить массогабаритные характеристики экранов.

Перспективными материалами являются пористые вспененные материалы: пеностекло, пенокерамика и ячеистые бетоны, которые вследствие специфики технологического процесса их изготовления позволяют производить добавление различных порошковых материалов для

улучшения их экранирующих характеристик. Так, добавление в диэлектрическую вспененную основу углеродосодержащих включений обусловливает высокие радиопоглощающие свойства этих материалов, а особенность структуры (наличие большого числа сообщающихся между собой полостей) обеспечивает высокий уровень звукопоглощения.

Целью работы является исследование звукоизолирующих и экранирующих свойств материалов, обладающих малой массой для создания многослойных интегральных защитных панелей на их основе.

Экспериментальная часть

Таким образом, для создания интегральных защитных конструкций требуется применение материалов, обладающих потерями для ЭМИ диапазона СВЧ, с неоднородной структурой, рассеивающей распространяющиеся волны, сформированной из нескольких слоев с различными микроволновыми и акустическими свойствами.

В качестве образцов для исследований использовались следующие материалы: образец А108, состоящий из двух слоев поролона, пропитанных 50%-й водной эмульсией шунгита и одного слоя алюминиевой фольги между ними; образец А109, состоящий из двух слоев поролона с нанесенным между ними слоем шунгита; образец А110 содержащий два слоя поролона с один слой порошкообразного шунгита герметизированного полиэтиленовой пленкой; образец А111 содержащий один слой поролона, пропитанного водой, с нанесенным на него слоем порошкообразного шунгита, и один слой сухого поролона (рис. 1). Все образцы были герметизированы полиэтиленовой пленкой.

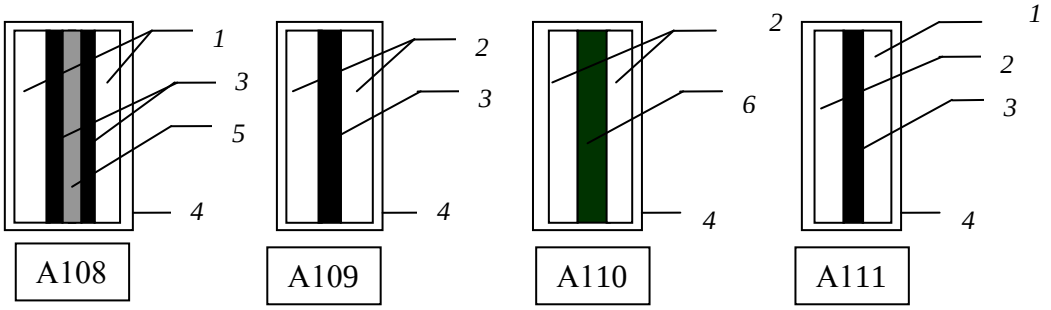


Рис. 1. Состав исследованных образцов: *1* – поролон, пропитанный водой; *2* – поролон сухой; *3* – шунгит; *4* – полиэтиленовая пленка; *5* – алюминиевая фольга, *6* – порошкообразный шунгит с добавлением воды, герметизированный полиэтиленовой пленкой

Исследование экранирующих свойств созданных образцов проводилось с помощью скалярных анализаторов цепей, позволяющих получить информацию о соотношениях амплитуд волн в измерительном тракте путем вычисления модулей комплексных элементов волновой матрицы рассеяния, описывающей линейный четырехполюсник [1], и волноводного измерительного тракта с рупорными антеннами. Эффективность экранирования ЭМИ исследуемыми конструкциями характеризуется величиной ослабления энергии ЭМИ и коэффициентом отражения электромагнитных волн от экрана. Измерения проводились в СВЧ диапазоне
0,7–140 ГГц с разделением диапазона на несколько поддиапазонов, охватываемых применяемой измерительной аппаратурой.

Звукоизоляция экспериментальных образцов измерялась на экспериментальной установке, описанной в работе [2]. Сигнал "белого шума", сформированный генератором, воспроизводился динамиком и излучался в трубу, все сечение которой перекрывает образец. Регистрация спектра сигнала за образцом осуществлялась микрофоном, соединенным с шумомером-спектроанализатором МАНОМ-4. Измерения проводились в третьоктавных полосах в частотном диапазоне от 200 до 8 000 Гц. Звукоизоляция рассчитывалась как разность уровней звукового давления при прямом прохождении звука и при прохождении звука через исследуемый образец.

Результаты и обсуждение

В результате серии экспериментов получены характеристики отражения и ослабления электромагнитного излучения материалами со структурой, содержащей включения шунгита. Использование слоя водосодержащего порошка шунгита (фракции ~0,1–0,2 мм) в комбинации с алюминиевой фольгой показало (рис. 2–3) возможность отражения ЭМИ до 25% и менее в диапазоне частот 1–150 ГГц, а применение отражателя из металла позволяет повысить эффективность ослабления до 1000 раз и более.

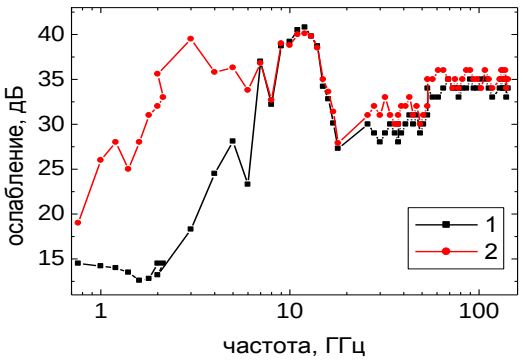


Рис. 2. Частотная зависимость ослабления электромагнитной волны: *1* – образцом А108; *2* – образцом А111

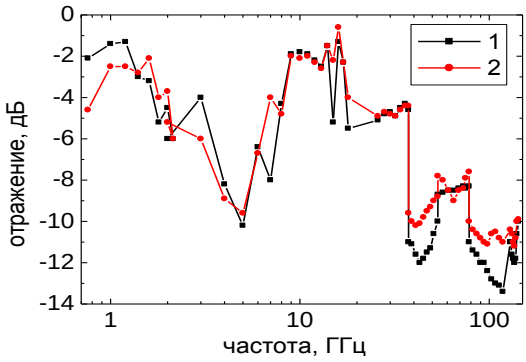


Рис. 3. Частотная зависимость коэффициента отражения электромагнитной волны: *1* – образцом А108; *2* – образцом А111

Показано (рис. 4), что образцы А110 и А108 ослабляют звук на 20 дБ в области частот от 160 до 2500 Гц. Начиная с частоты 2500 Гц и заканчивая частотой 8000 Гц, значение звукоизоляции возрастает с 20 до 70 дБ. Образцы А109 и А111 в области частот от 160 до 2500 Гц ослабляют звук примерно на 10 дБ. Максимальный уровень ослабления звука для образца А111 составляет 30 дБ, а для образца А110 — 50 дБ в полосе частот со среднегеометрической частотой 8000 Гц.

Учитывая то, что низкочастотная составляющая речи несет в себе основную энергию речевого сигнала, ослабление сигнала на 20 дБ в области частот до 2500 Гц несущественно скажется на разборчивости речи, прошедшей через такую конструкцию. Такой результат объясняется малой толщиной исследуемых образцов (примерно 2 см). Сочетание жестких и мягких слоев, а так же увеличение массы позволит получить более высокое значение собственной звукоизоляции

Из рис. 5 видно, что добавление к многослойной панели на основе стекломагнезита панели, состоящей из последовательно расположенных образцов А108 – А111 привело к увеличению собственной звукоизоляции получившейся конструкции на 10 дБ в области частот 1000–3500 Гц по сравнению с конструкцией, содержащей только образцы А108 – А111, и к увеличению на 20 – 30 дБ в диапазоне частот 1250…8000 Гц по сравнению с многослойной конструкцией на основе стекломагнезитовой плиты.

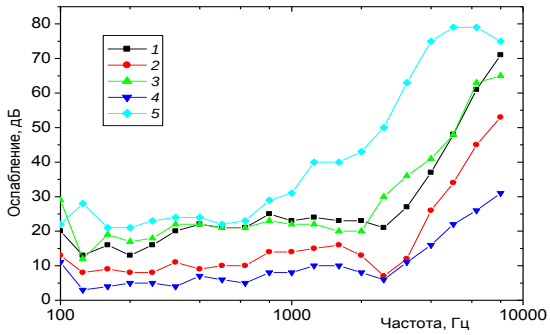


Рис. 4. Зависимость ослабления воздушного шума от частоты многослойными панелями: *1* – А 108; *2* – А109; *3* – А110; *4* – А111; *5* – образцы А108–А111 сложенные вместе

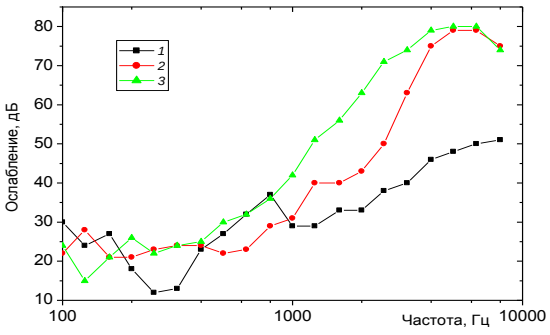


Рис. 5. Зависимость ослабления воздушного шума от частоты: *1* – лист стекломагнезита толщиной 4 мм, слой резины толщиной 1 мм, алюминиевая фольга толщиной ~0,4 мм; *2* – образцы А108–А111 сложенные вместе; *3* – панель 1 и образцы А108-А111 (мягкие слои обращены к динамику)

Заключение

Исследованы электромагнитные и акустические характеристики материалов на основе шунгита для создания панелей интегральной защиты. Показана возможность создания многослойных материалов для защищенных помещений на основе модульных разборных конструкций, в том числе и из оптически прозрачных элементов.

MULTILAYERED FOAM MATERIALS BASED ON SHCUNGITE FOR PASSIVE COMPLEX SECURITY SYSTEMS

H.M. ALLEBAD, S.N. PETROV, A.M. PROUDNIK

Abstract

The measurements results of the electromagnetic and acoustic properties of multilayered structures based on water-containing materials and schungite for complex security systems are given. The creation possibility of multilayered panels with the value of electromagnetic wave attenuation over 30 dB и isolation indexes of air noise 35 dB is shown.

Литература

1. *Прудник А.М., Петров С.Н., Лыньков Л.М.* // Управление защитой информации. 2009. Т. 13, № 1. С. 67–70.
2. *Богуш В.А., Борботько Т.В., Гусинский А.В. и др.* Электромагнитные излучения. Методы и средства защиты. М., 2003.

УДК 004.622+004.934+534.86=411.21

ФОРМИРОВАНИЕ БАЗ ДАННЫХ НА РУССКОМ ЯЗЫКЕ ДЛЯ ВЕРИФИКАЦИИ АРАБСКОЯЗЫЧНЫХ ДИКТОРОВ

М.О. АЛЬ-ХАТМИ, М.Ш. МАХМУД, Л.М. ЛЫНЬКОВ, А.Г. ДАВЫДОВ, Д.А. БОРИСЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки,6, Минск, 220013, Беларусь

Поступила в редакцию 5 октября 2009

Рассмотрены принципы построения и описаны базы данных на русском языке для возможного распознавания речи дикторов арабского происхождения, учитывающие артикуляционные отличия согласных и гласных звуков русского и арабского языков и результаты измерений статистических спектральных характеристик.

Ключевые слова: речь, диктор, спектр, артикуляция.

Введение

При оценке принадлежности диктора к какой-либо этнической группе (национальности) используются экспертные методики определения разборчивости речевых сигналов, в частности по артикуляционным таблицам [1], которые представляют собой измерения относительного числа правильно переданных слов, слогов и звуков через испытываемый (тестируемый) канал. Разрабатываемая методика формирования баз данных на русском языке, используемая диктором – носителем арабской речи, в первую очередь предназначается для систем распознавания русскоязычной речи для экспертных систем, систем оценки и улучшения качества связи, анализа речи возможных террористов и злоумышленников [2].

Целью данной работы является разработка методологических основ и составление артикуляционных таблиц на русском языке путем сравнения систем согласных и гласных звуков арабского и русского языков [3], различий в статистических характеристиках спектра речи для оценки ее разборчивости и идентификации.

Органы речи и классификация речи

Звуки речи образуются с помощью речевого аппарата. Органы, составляющие речевой аппарат человека, делятся на: 1) дыхательные органы (легкие, бронхи, дыхательное горло); 2) гортань с голосовыми связками; 3) надгортанные полости. Дыхательные органы подают струю воздуха, необходимого для образования звука, которая попадает в гортань, где находятся голосовые связки. Последние представляют собой две мускульные складки. Когда голосовые связки сближены и напряжены, струя воздуха, проходящая между ними, с силой раздвигает их и приводит в колебания, в результате чего образуется музыкальный тон (голос).

Надгортанные полости состоят из полости глотки, полости рта и полости носа. Работа органов речи при образовании звуков речи называется артикуляцией. В зависимости от того, какое участие органы речи принимают в образовании звуков, они делятся на активные (подвижные) и пассивные (неподвижные).

Активные органы речи, к которым относятся губы, язык, язычок, голосовые связки и мышцы гортани, определяют звуки по способу их артикуляции.

Пассивные органы речи, к которым относятся зубы, нёбо и гортань, определяют звуки по месту их артикуляции.

Кроме классификации звуков речи с точки зрения физиологической, их можно также классифицировать с точки зрения акустической, т.е. по тому, какое впечатление на слух производит тот или иной звук.

Все звуки речи делятся, прежде всего, на согласные и гласные.

Согласные звуки

В основе артикуляции согласных звуков лежит шум, образуемый в полости рта или гортани. По способу артикуляции согласные звуки делятся на: смычные (мгновенные), например, русские *д, т* ; щелевые (фрикативные), например, русские *с ,з*; и смычно-щелевые (аффрикаты). Аффрикаты – это сложные звуки, в которых первый образующий их звук смычный, а второй – фрикативный. В русском языке, например, аффрикатой является звук *ч*, состоящий из звука *т*, произносимого с последующим звуком *ш* слитно.

В табл. 1 представлена классификация согласных звуков арабского языка [4].

Таблица 1. **Классификация согласных звуков арабского языка**

По способу артикуляции \ По месту артикуляции			Губные		Нёбные						Гортанные	
					Передненёбные				Средненёбные	Глубокозаднебные	Связочные	Зев-ные
			Губно-	Губно-	Межзубные	Зазубные (простые)	Зазубные (эмфатические)					
Смычные	Шумные взрывные	Звонкие	б			д	д̣					ʿайн
		Глухие				т	т̣		к	қ	ʾхамза	
	Сонанты носовые		м					н				
Щелевые (фрикативные)	Шумные	Звонкие			з̲	з	з̣			ғ		
		Глухие		ф	с̲	с	с̣	ш		х̲	х	х̣
	Сонанты		ў					л	й			
Смычно-щелевые (аффрикаты)		Шумные звонкие						дж				
Дрожащие (вибранты)		Сонанты						р				

По месту артикуляции согласные делятся на губные (губно-губные, губно-зубные), нёбные (передненёбные, средненёбные, глубоко-задненёбные), гортанные (связочные и зевные).

Артикуляция согласных характеризуется наличием:

– шума;

– музыкального тона (голоса). В зависимости от наличия голоса согласные делятся на глухие и звонкие;

– палатализации, т.е. смягчения. Согласные, подвергающиеся смягчению, называются палатализованными;

– эмфатичности (напряженности звука). Звуки, произносимые с напряжением, называются эмфатическими (или зычными).

И, наконец, в зависимости от того, что преобладает при артикуляции согласного звука – шум или голос, согласные делятся на шумные (например, русские *б, с, з*) и сонорные (*м, р, н, л*).

Сравнение системы согласных звуков арабского и русского языков показывает, что между ними имеются существенные различия: 1) в русском языке 35 согласных звуков, а в

арабском – 28; 2) в большинстве своем русские согласные различаются по признаку мягкости и твердости, чего в арабском языке не наблюдается; 3) в арабском языке есть такие согласные звуки, которых нет в русском языке (например, межзубные, эмфатические, зевные и др.); с другой стороны в русском языке есть такие согласные звуки, которых нет в арабском языке (например: *п, в, ц, ч* и др.)

Гласные звуки

Основой артикуляции гласных звуков является музыкальный тон (голос). Гласные звуки классифицируются в зависимости от положения основных органов речи, участвующих при их образовании: языка, губ и мягкого нёба. В зависимости от положения языка в полости рта гласные звуки различаются по ряду и степени подъема языка. По ряду гласные классифицируются на гласные заднего, среднего и переднего ряда. По степени подъема языка различаются гласные нижнего, среднего и верхнего подъема (например, русская *а* – нижнего подъема, переднего ряда). Губы при артикуляции гласных либо округлены (лабиализованы), либо находятся в нейтральном положении. В зависимости от положения губ гласные делятся на лабиализованные (например, русские *о, у*) и нелабиализованные (например, русские *а, и*).

В зависимости от степени раскрытия рта гласные подразделяются на гласные открытого типа (например, русская *а* в слове «база») и гласные закрытого типа (например, русская *и* в слове «милый»).

Помимо приведенной выше классификации гласных звуков в качественном отношении, в арабском языке гласные различаются также количественно, т.е. по признаку долготы и краткости, причем этот признак имеет смыслоразличительное значение.

Другой фонетической особенностью арабского языка является то, что в нем не допускается стечение двух гласных, стоящих рядом (например, как в слове «сообщение»).

Разработка принципов построения и описания баз данных на русском языке для сегментации речевых сигналов арабскоязычных дикторов

Для возможного автоматизированного распознавания дикторов арабского происхождения, которые произносят речь на русском языке, предлагается следующая схема построения (рис. 1) на основе расчета и измерения ее разборчивости.

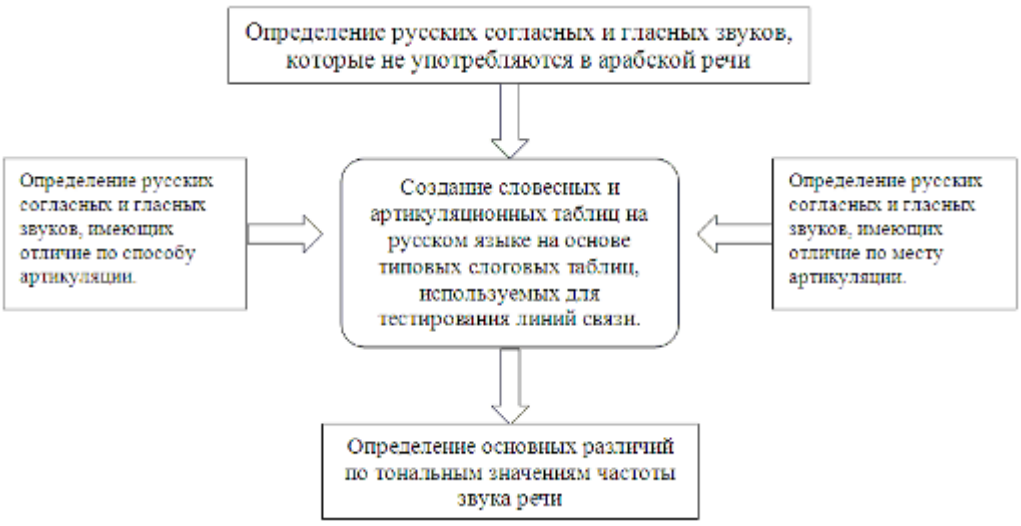


Рис 1. Схема построения методики анализа речи на русском языке, произносимой арабскоязычным диктором.

Первый этап построения такой методики заключается в определении русских согласных и гласных звуков, имеющих отличие по месту артикуляции. Второй этап характеризуется

определением русских согласных и гласных звуков, которые не употребляются в арабской речи. На третьем этапе проводится анализ русскоязычных текстовых таблиц [3] и их направленный выбор для оценки разборчивости речи.

Основной особенностью данной методики является установление и учет распределения звукового давления такой речи по октавным полосам.

Статистические характеристики спектра речи

Анализ статистических характеристик спектра речи по литературным источникам показывает, что имеются различия спектров в зависимости от языка. В связи с этим была проведена работа по изучению различий в спектре речи разных языков, так как эти данные могут быть использованы при оценке разборчивости речи в каналах связи и построении систем защиты речевой информации для каждого конкретного языка.

При изучении статистических характеристик речи использовались аудиозаписи с речью дикторов, которые являются носителями данных языков. Запись аудиозаписей выполнялась на персональном компьютере с помощью аппаратуры RFT для акустических измерений с линейной частотной характеристикой в диапазоне 20 Гц – 10 кГц и программы Sound Forge 9.0. Предварительная обработка аудиофайлов проходила с использованием программы Sound Forge 9.0. Запись дикторов из Беларуси и арабских стран проводилась в акустически заглушенной комнате. Данные по русской и английской речи были взяты из литературных источников [2], [3].

Построение спектра речевых сигналов и дальнейшее изучение различий спектров проводилось с помощью программы MatLAB R2008. В данной программе получали значение мощности всего сигнала и характеристики звукового давления по октавам. Так как аудиозаписи разных дикторов были получены с разными интегральными уровнями, полученные данные нормировались на один уровень – 70 дБ. Статистическая обработка проводилась на основании полученных данных и посчитанных средних значений [5,6].

Для подсчета средних значений данные уровней звукового давления, выраженного в децибелах, переводились в значение звукового давления, выраженного в паскалях, по формуле:

$$P = 10^{(\bar{P}/20)} \cdot P_0, \qquad (1)$$

где P – полученное значение уровня звукового давления, дБ; P_0 – пороговый уровень слуха, равный $2 \cdot 10^{-5}$ Па.

Далее для всех значений P одной октавы находилось среднее значение звукового давления $P_{\text{ср}}$. Средние значения звукового давления $P_{\text{ср}}$ затем переводились в звуковое давление, выраженное в децибелах.

Для оценки полученных результатов и задания доверительного интервала была посчитано среднеквадратичное отклонение σ в каждой октаве по формуле:

$$\sigma = \sqrt{\frac{\sum_{i=n}^{n} (P_i - P_{cp})^2}{n}}, \qquad (2)$$

где P_i - значение звукового давления в октаве для i-го диктора, Па; i – для всех дикторов, представителей одного языка; n – количество дикторов.

В табл. 2 представлены полученные результаты анализа спектров речи для различных языков. В графе «белорусская» представлены спектры жителей Республики Беларусь, которые читали текстовые таблицы Д50 и Д70 на русском языке из СТБ ГОСТ Р50840-2000. Также на рис. 2–5 представлены графики с распределением звукового давления по октавам для каждого языка отдельно. На приведенных графиках видно, что статистические характеристики речи разных языков различны. При оценке разборчивости речи в каналах связи и построении систем защиты речевой информации необходимо учитывать полученные данные. При построении более точных систем можно использовать характеристики звукового давления по третьоктавным полосам, которые являются более точными.

Таблица 2. **Распределение звукового давления по октавным полосам**

Речь	Среднее значение звукового давления, дБ				
	1-я октава, $f_{ср}$=250 Гц	2-я октава, $f_{ср}$=500 Гц	3-я октава, $f_{ср}$=1000 Гц	4-я октава, $f_{ср}$=2000 Гц	5-я октава, $f_{ср}$=4000 Гц
белорусская	$P_{ср}$=65,4 $P_{ср}+\sigma_+$=66,6 $P_{ср}-\sigma_-$=63,9	$P_{ср}$=67,1 $P_{ср}+\sigma_+$=68,0 $P_{ср}-\sigma_-$=66,0	$P_{ср}$=59,0 $P_{ср}+\sigma_+$=61,5 $P_{ср}-\sigma_-$=55,7	$P_{ср}$=55,2 $P_{ср}+\sigma_+$=57,6 $P_{ср}-\sigma_-$=52,0	$P_{ср}$=50,4 $P_{ср}+\sigma_+$=52,9 $P_{ср}-\sigma_-$=46,7
русская [2]	66,3	66,0	60.8	56,1	53,0
арабская	64,8	64,2	63,2	57,9	49,8
английская [3]	65,1	67,0	62,6	53,7	44,0

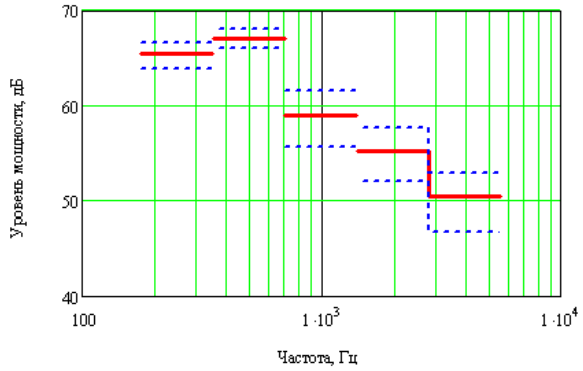


Рис. 2. Белорусская речь

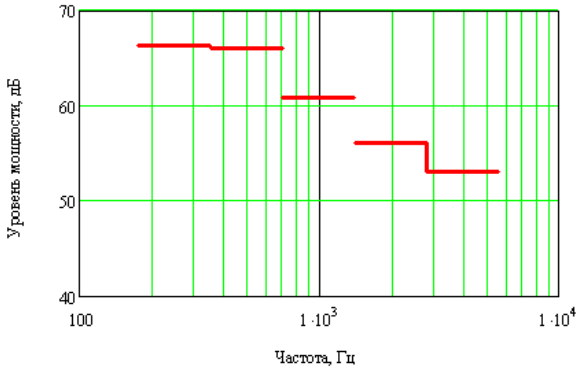


Рис. 3. Русская речь

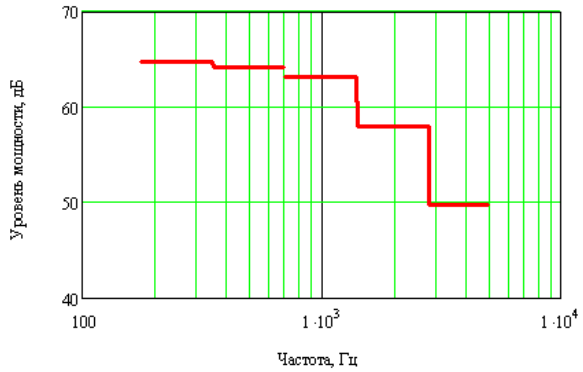


Рис. 4. Арабская речь

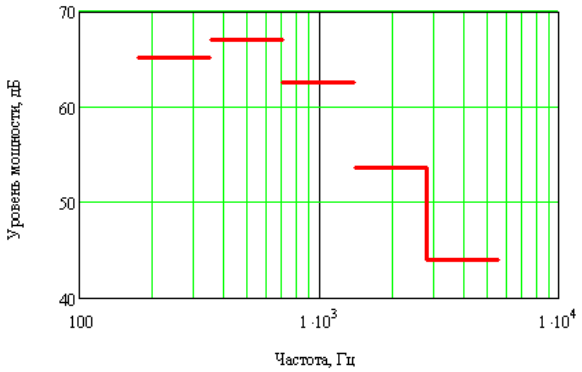


Рис. 5. Английская речь

Заключение

В результате сравнения системы согласных и гласных звуков русского и арабского языков показаны их различия по принципу мягкости и твердости. При этом в русском языке употребляются такие согласные звуки, которых нет в арабском языке, что позволило создать словесные и артикуляционные таблицы на русском языке для арабскоязычных дикторов. Экспериментально установлена значительная разница в статистических спектральных характеристиках речи по октавам для каждого языка.

FORMATION OF DATABASES IN RUSSIAN LANGUAGE FOR ARABIC ANNOUNCER SPEECH SIGNALS VERIFICATION

M.O. ALHATME, M.SH. MAHMOUD, L.M. LYNKOU, A.G. DAVIDOV, D.A. BORISEVICH

Abstract

The database in Russian for possible speech recognition of Arabic announcer is described and principles of its construction are considered. These databases take into account the articulation differences of consonants and vowels in Russian and Arabic languages. The results of statistical measurements of spectral characteristics are used.

Литература

1. *Михайлов В.Г., Златоустова Л.В.* Измерение параметров речи. М., 1987.
2. *Хорев А.А.* Защита информации от утечки по техническим каналам. Ч.1. Технические каналы утечки информации . /Учебное пособие. М., 1998.
3. *Покровский Н.Б.* Расчет и измерение разборчивости речи. М., 1962.
4. *Ковалев А.А., Шарбатов Г.Ш.* Учебник арабского языка. М., 1979.
5. Железняк В.К., Макаров Ю.К., Хореев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации.
6. ISO/TR4870 Acoustics – The construction and calibration of speech intelligibility test. P. 22.

Статьи рекомендованы к публикации Международным научно-техническим семинаром – ТЕЛЕКОММУНИКАЦИИ: СЕТИ И ТЕХНОЛОГИИ, АЛГЕБРОИЧЕСКОЕ КОДИРОВАНИЕ И БЕЗОПАСНОСТЬ ДАННЫХ

Сведения об авторах

1.	Аль-Алем Ахмед Саид	− аспирант кафедры сетей и устройств телекоммуникаций БГУИР
2.	Альлябад Хуссейн Мухаммед	− аспирант кафедры защиты информации БГУИР
3.	Аль-Джубури Тарик	− аспирант кафедры сетей и устройств телекоммуникаций БГУИР
4.	Аль-Фурайджи Одай Джасим	− аспирант кафедры сетей и устройств телекоммуникаций БГУИР
5.	Аль-Хайдар Елена Касимовна	− аспирант кафедры высшей математики БГУИР
6.	Аль-Хатми Мохаммад Омар	− аспирант кафедры защиты информации БГУИР
7.	Бобов Михаил Никитич	− д.т.н., профессор, начальник отдела безопасности НИИСА
8.	Борисевич Дмитрий Анатольевич	− студент БГУИР
9.	Давыдов Андрей Геннадьевич	− к.т.н., стар. научн. сотр. Академии управления
10.	Козловский Владимир Владимирович	− ведущий специалист Информационно-аналитического центра при Администрации Президента Республики
11.	Конопелько Валерий Константинович	− д.т.н., профессор, зав. кафедрой СиУТ БГУИР
12.	Конопелько Иван Валерьевич	− соискатель БГУИР
13.	Королев Алексей Иванович	− к.т.н., доцент кафедры СиУТ БГУИР
14.	Курилович Андрей Владимирович	− зам. директора учебного центра «Связьинвест»
15.	Липницкий Валерий Антонович	− д.т.н., профессор кафедры высшей математики БГУИР
16.	Лыньков Леонид Михайлович	− д.т.н., профессор, зав. кафедрой ЗИ БГУИР
17.	Макейчик Екатерина Геннадьевна	− ассистент кафедры СиУТ БГУИР
18.	Махмуд Мухаммед Ш.	− магистрант кафедры ЗИ БГУИР
19.	Мохаммед Файсал Осман Мохаммед	− аспирант кафедры СиУТ БГУИР
20.	Петров Сергей Николаевич	− аспирант кафедры ЗИ БГУИР
21.	Прудник Александр Михайлович	− к.т.н., доцент кафедры экологии БГУИР
22.	Смолякова Ольга Георгиевна	− аспирант кафедры СиУТ БГУИР
23.	Цветков Виктор Юрьевич	− к.т.н., доцент кафедры СиУТ БГУИР
24.	Чесалин Николай Владимирович	− аспирант кафедры СиУТ БГУИР
25.	Шкиленок Александр Владимирович	− ведущий инженер НИИ ТЗИ, ассистент кафедры ЗИ БГУИР
26.	Pham Khac Hoan	− Le Quy Don Technical University, Ha noi, Viet Nam
27.	Dang Xuoan Hai	− Le Quy Don Technical University, Ha noi, Viet Nam
28.	Vu Son Ha	− Institute of Information Technology, Ha noi, Viet Nam