ИНФОРМАЦИОННЫЕ СИСТЕМЫ. СРЕДСТВА, ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ

ВЛИЯНИЕ СПОСОБА ПАРАМЕТРИЗАЦИИ НА ЭФФЕКТИВНОСТЬ НЕЙРОСЕТЕВОГО ДЕТЕКТИРОВАНИЯ ФАЗОМАНИПУЛИРОВАННЫХ СИГНАЛОВ

О.А. Морозов, П.Е. Овчинников, Ю.А. Сёмин

Нижегородский госуниверситет

Искусственные нейронные сети могут быть использованы при построении систем обработки сигналов различной природы, в том числе и радиосигналов. В данной работе рассматривается метод детектирования фазоманипулированных (ФМ) сигналов при помощи многослойной нейронной сети. Поскольку дискриминационные возможности нейронной сети ограничены [1], эффективность обработки существенно зависит от способа параметризации исходного сигнала. В работе проведено сравнение эффективности детектирования для разных способов параметризации.

Если сформулировать задачу детектирования ФМ-сигнала как задачу распознавания моментов изменения фазы, то для детектирования может быть построена следующая схема. В качестве решающего устройства используется многослойный персептрон [1], на его вход подаются вычисленные характеристики детектируемого сигнала. По выходам персептрона определяются вероятности манипуляций (скачкообразных изменений фазы сигнала). Число выходов персептрона равно числу возможных изменений фазы, в частности для ФМ-4 сигнала оно равно четырем. Тип манипуляции (величины изменения фазы) определяется по выходу нейросети с максимальным значением, то есть как наиболее вероятный. Чтобы увеличить устойчивость метода детектирования к шуму, вычисление параметров сигнала и последующая нейросетевая обработка производятся для нескольких соседних по времени участков сигнала. Участки сигнала перекрываются и относятся к одному передаваемому символу, т.е. содержат одну манипуляцию, это позволяет принимать решение о передаваемом символе по усредненным значениям вероятностей. Детектирование осуществляется при помощи обученного персептрона, набор данных для обучения и число входов персептрона определяются способом параметризации. В работе сравнены следующие способы параметризации: 1) на вход сети подаются отсчеты реализации ФМ-сигнала (самый простой способ параметризации); 2) на вход сети подаются отсчеты синфазной (I) и квадратурной (Q) компонент сигнала (например, с выхода цифрового приёмника); 3) на вход сети подаются отсчеты фазы сигнала, вычисленной по IQ-компонентам.

Для отыскания оптимального для нейросети способа параметризации ФМ-сигнала был проведен сравнительный эксперимент. Поскольку исходная информация (ФМ-сигнал) и нейронная сеть были одинаковыми для всех способов параметризации, то по результатам сравнения эффективности распознавания можно судить

об адекватности того или иного способа задаче детектирования. Нейронная сеть обучалась отдельно для каждого способа параметризации, после чего для определения вероятности ошибки производилось детектирование ФМ-сигналов с разными соотношениями сигнал/шум.

Результаты статистических экспериментов по детектированию представлены на рисунке, где изображены зависимости вероятности символьной ошибки от соотношения сигнал/шум для исследованных способов параметризации. Видно, что применение IQ-компонент обеспечило наибольшую эффективность детектирования.

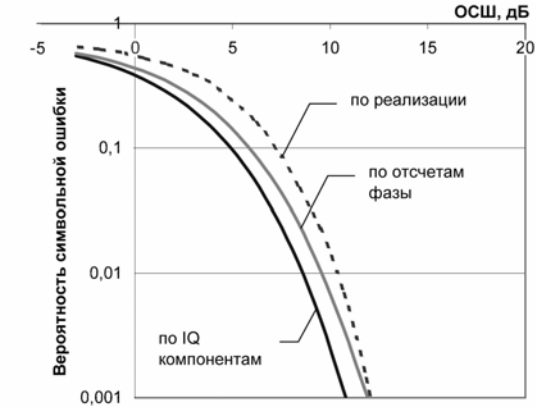

Рис.

Таким образом, в настоящей работе представлен метод детектирования фазоманипулированных сигналов с применением нейронной сети. Проведено компьютерное моделирование для сигналов ФМ-4. Проведенное сравнение различных методов параметризации показало, что наиболее подходящим для детектирования является вычисление IQ-компонент и использование их отсчётов в качестве входных параметров нейронной сети.

[1] Головко В.А. Нейронные сети: обучение, организация и применение. М.: ИПРЖР, 2001. 256 с.

О ПРИМЕНЕНИИ ТЕОРИИ ИНВАРИАНТНОСТИ ПРИ СИНТЕЗЕ МАТЕМАТИЧЕСКИХ МОДЕЛЕЙ КРИПТОСИСТЕМ

К.Г. Кирьянов, А.А. Горбунов, И.С. Зотов

Нижегородский госуниверситет

При построении математических моделей (ММ) криптосистем (КС) обнаруживаются их общие черты с системами автоматического управления, основанными на принципе компенсации Г.В. Щипанова (теории инвариантности) [1]. Как было показано ранее, в дискретных динамических системах (ДДС), как и в непрерывных системах, можно достигнуть проявления эффекта компенсации, а также перейти от общей структурной схемы КС к подобной инвариантной системе [2].

Для получения унифицированного вида ММ КС предложен подход, основанный на описании блоков шифратора и дешифратора КС в виде q-уровневых линей-

ных цифровых автоматов (ЛЦА). Системы уравнений ЛЦА в *ABCD*-форме для шифратора, канала связи без задержки и дешифратора записываются в виде [3]:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(0) = x_0 \end{cases}, \quad y(t) = u^*(t), \quad \begin{cases} x^*(t+1) = A^* x^*(t) + B^* u^*(t) \\ y^*(t) = C^* x^*(t) + D^* u^*(t) \\ x^*(0) = x_0^* \end{cases}. \tag{1}$$

Здесь входным сигналом $u(t)$ является открытый текст, сигналом $y(t) = u^*(t)$ – шифротекст, сигналом $y^*(t)$ – восстановленное сообщение (рис. 1). Условие восстановления исходного сообщения по шифротексту внутри КС записывается как

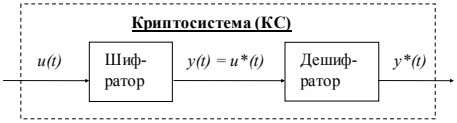

Рис. 1

$$u(t) \equiv y^*(t). \tag{2}$$

Данное условие соответствует условию компенсации входного сигнала $u(t)$ в модифицированной (инвариантной) системе (рис. 2), получаемой из данной КС:

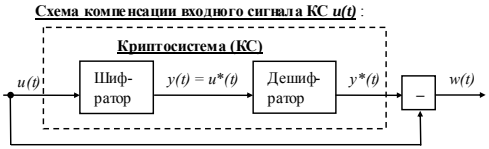

Рис. 2

$$w(t) = u(t) - y^*(t) \equiv 0. \tag{3}$$

Целью настоящей работы является получение условий восстановления открытого текста по шифротексту дешифратором КС из условия инвариантности модифицированной ДДС (рис. 2).

Совокупная ММ инвариантной ДДС, получаемой из модели КС (1), может быть также представлена в виде ЛЦА с совместным вектором состояния $[x(t) \mid x^*(t)]^T$:

$$\begin{cases} x(t+1) = Ax(t) + Bu(t) \quad ; \quad x^*(t+1) = B^* Cx(t) + A^* x^*(t) + B^* Du(t) \\ w(t) = D^* Cx(t) + C^* x^*(t) + D^* Du(t) - u(t) \quad ; \quad x(0) = x^*(0) = x_0 \end{cases}. \tag{4}$$

Введением символа p динамического оператора задержки на один такт для случая дискретных алгебраических структур (АС) (например, $GF(q)$)

$$px(t) = x(t+1) \tag{5}$$

(аналогом данного оператора в "частотной" области дискретного z-преобразования является операция умножения на z^{-1}) можно свести систему разностных уравнений (4) к стандартному операторному виду систем динамических (дифференциальных, разностных) уравнений, принятому в теории инвариантности:

$$\begin{cases} [p - A]x(t) & & & = & [B]u(t) \\ [-B^* C]x(t) & + & [p - A^*]x^*(t) & = & [B^* D]u(t) \\ [-D^* C]x(t) & + & [-C^*]x^*(t) + [E]w(t) & = & [D^* D - E]u(t) \end{cases}. \tag{6}$$

Для нахождения условий инвариантности переменной $w(t)$ по отношению к внешнему воздействию $u(t)$ необходимо разрешить (6) как систему алгебраических уравнений (операторный метод) относительно $w(t)$ и приравнять нулю получившийся в результате операторный многочлен относительно p:

$$w(t)=\frac{\Delta w}{\Delta}:\ \Delta w=\begin{vmatrix}[p-A] & [0] & [B]\\ [-B^*C] & [p-A^*] & [B^*D]\\ [-D^*C] & [-C^*] & [D^*D-E]\end{vmatrix}u(t)=0\ ,\ \Delta=\begin{vmatrix}[p-A] & [0] & [0]\\ [-B^*C] & [p-A^*] & [0]\\ [-D^*C] & [-C^*] & [E]\end{vmatrix}=[p-A]\times\ \times[p-A^*]\neq 0\ . \quad (7)$$

В результате преобразований (7) выражение для Δ_w принимает следующий вид:

$$\Delta w=\begin{Bmatrix}[D^*D-E]p^2-[D^*D-E][A+A^*]p+[BD^*C+B^*DC^*]p+\\ +[D^*D-E][AA^*]-[BD^*CA^*]-[B^*DC^*A]+[BB^*CC^*]\end{Bmatrix}u(t)\ , \quad (8)$$

из которого видно, что выполнение условия инвариантности (3) накладывает следующие условия на матрицы ММ КС:

$$\begin{cases}[D^*D-E]=[0]\\ [BD^*C+B^*DC^*]=[D^*D-E][A+A^*]\\ [BB^*CC^*]-[BD^*CA^*]-[B^*DC^*A]=[D^*D-E][AA^*]\end{cases}\ \text{или}\ \begin{cases}\exists D^{-1}:\ D^*=D^{-1}\\ B^*DC^*=-BD^{-1}C\\ BB^*CC^*=BD^{-1}CA^*+B^*DC^*A\end{cases}\ . \quad (9)$$

Данные уравнения полностью удовлетворяются при выполнении полученных ранее условий восстановления открытого текста по шифротексту [3]:

$$A^*=A-BD^{-1}C,\ B=BD^{-1},\ C^*=-D^{-1}C,\ D^*=D^{-1},\ x_0{}^*=x_0. \quad (10)$$

Полученные соотношения для КС и родственных им инвариантных ДДС были проверены компьютерным экспериментом при синтезе ММ для ряда классических систем шифрования (шифр Вижинера, шифрование гаммированием и др.).

[1] Г.В. Щипанов и теория инвариантности (Труды и документы) / Сост. З.М. Лезина, В.И. Лезин. М.: Физматлит, 2004.
[2] Кирьянов К.Г., Горбунов А.А. // Труды 7 Всероссийской научной конференции «Нелинейные колебания механических систем». Н. Новгород: ННГУ, 2005. С. 308.
[3] Горбунов А.А., Кирьянов К.Г. // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Радиофизика. Н.Новгород: Изд-во ННГУ. 2004. Вып. 1(2). С. 24.

ЭКСПЕРИМЕНТАЛЬНЫЙ АНАЛИЗ ПАРАМЕТРОВ СТОЙКОСТИ КРИПТОСИСТЕМ

К.Г. Кирьянов, А.А. Попов

Нижегородский госуниверситет

Разработана экспериментальная программная система (ПС) для структурной идентификации и сравнения шифраторов криптосистем (КС) рис. 1 по стойкости. В

настоящее время нам неизвестны строгие доказуемые оценки стойкости для многих используемых на практике шифров. Поэтому стойкость в ПС оценивается по функции ненадёжности (ФН) (1) и расстоянию единственности (РЕ) (2) К.Шеннона [1], которые, как показано в [2], выражаются через измеряемые в доступных контрольных точках КС т.н. базовые параметры (БП) входных и выходных процессов [3] по формулам:

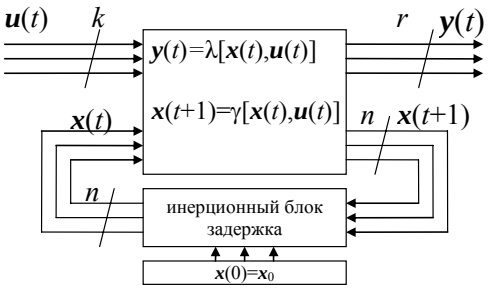

Рис. 1

$$E(u \mid y) = E(uy) - E(y) = n_{uy}(k+r)\log q_{uy} - n_y r \log q_y \,, \tag{1}$$

$$n^* = [n_{uy}(k+r)\log q_{uy}]/[r \log q_y] = [E_{uy}/E_y]\cdot n_y \,. \tag{2}$$

Здесь k и r – размерности векторного входа и выхода, n_y, q_y, n_{uy}, q_{uy}– БП выходного и совместного процессов и энтропия $E_y=n_y r\log q_y$.

ПС производит анализ стойкости по РЕ как ряда стандартных блочных (например, *CAST*128), так и экспериментальных поточных линейных КС, приведённых к «*ABCD*-форме» в алгебраической структуре $GF(q)$ [4]:

$$\begin{cases} \boldsymbol{X}(t+1) = A\boldsymbol{X}(t) + B\boldsymbol{U}(t) \\ \boldsymbol{Y}(t) = C\boldsymbol{X}(t) + D\boldsymbol{U}(t) \\ \boldsymbol{X}_0 = X(0) \end{cases} . \tag{3}$$

Здесь вектор $\boldsymbol{X}(t)$ –состояние шифратора в моменты времени t=0,1,2,…, а $\boldsymbol{U}(t)$ и $\boldsymbol{Y}(t)$ – векторные процессы на входе и выходе, $\boldsymbol{X}_0$ – начальное состояние. Параметры шифратора задаются вводом матриц $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$, $\boldsymbol{D}$ и вектора $\boldsymbol{X}_0$. Вектор $\boldsymbol{U}(t)$ формируется из входных файлов. Ключами в поточных КС в форме (3) могут являться как матрицы автомата, его начальное состояние, так и компоненты векторного входного процесса. Для КС (3) возможен ручной ввод матриц. Для моделей КС, приведённых к *ABCD*-форме, матрицы задаются указанием шифра (Цезаря, Вижинера, гаммирование и т.д.). Дешифрование КС производится по формулам [4]:

$$\boldsymbol{D}^*=\boldsymbol{D}^{-1},\ \boldsymbol{A}^*=A-BD^{-1}\boldsymbol{C},\ \ \boldsymbol{B}^*=BD^{-1},\ \boldsymbol{C}^*=-D^{-1}\boldsymbol{C},\ \ \boldsymbol{X}_0^*=X_0. \tag{4}$$

Для любого вида КС исходные и полученные файлы, параметры режима работы сохраняются в отдельной папке с уникальным именем и передаются в блок ана-

лиза для измерения БП и их функционалов: ФН, РЕ и других параметров КС (см. таблицу).

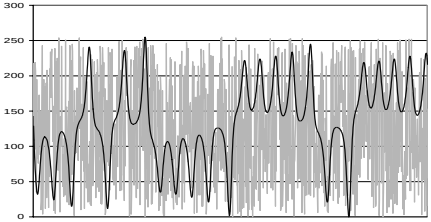

Рис. 2

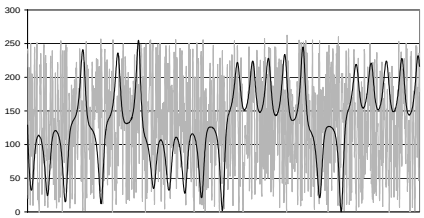

Рис. 3

q	q_u	n_u	q_y	n_y	q_{uy}	n_{uy}	E_u	E_y	E_{uy}	E_{uy}/E_y	$E(u\|y)$	n^*
256	183	9	120	3	76	3	68	21	37	1,76	17	5
128	104	12	90	4	64	3	80	26	36	1,38	10	6
26	13	45	2	112	5	36	167	112	167	1,49	55	167

q	q_u	n_u	q_y	n_y	q_{uy}	n_{uy}	E_u	E_y	E_{uy}	E_{uy}/E_y	$E(u\|y)$	n^*
2^{32}	1026	3	53	3	415	1	30	17,2	17,4	1,01	0,21	3,0
2^{16}	1026	3	319	2	756	1	30	16,6	19,1	1,15	2,45	2,3
2^8	183	9	63	3	48	2	68	17.9	22.3	1.24	4.4	3.7

Большое число параметров анализа позволяет оценивать различные характеристики шифраторов, входных и выходных процессов. Например, при шифровании файла с 1001 отсчётом (т.е., r=1, k=1) графики проквантованного на q=256 уровней исходного процесса $\boldsymbol{U}(t)$ и $\boldsymbol{Y}(t)$, зашифрованного поточным алгоритмом (3) гаммированием (с ключом «15 17 a=21 b=18») и блочным *CAST128* (с ключом *«59dc083d1e»*), показаны соответственно на рис. 2 и рис. 3, вместе с таблицами результатов анализа.

В каждой из таблиц отношение E_{uy}/E_y (см. (2)) показывает, во сколько раз n^* должно быть больше n_y, чтобы в (1) $E(\boldsymbol{U}|\boldsymbol{Y})$=0. Как показано в [2], n^* это оценка минимального размера шифротекста, по которому однозначным образом восстанавливается оставшийся шифротекст на участке одного гена. Значения РЕ и ФН зависят от самих процессов $\boldsymbol{U}(t)$ и $\boldsymbol{Y}(t)$ на входе и выходе шифратора, а значит, от используемых криптоалгоритмов, от длины и значений ключей, от выбранной точности шифрования q. Параметр q влияет на сигналы как на входе, так и на выходе шифратора. Из алгоритма поиска БП [3] следует, что для скалярного случая отношение E_{uy}/E_y не больше 2 и n^* всегда порядка n_y, а также что n_y тем больше, чем меньше q_y ($q_y<q$).

[1] Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. М.: ИЛ, 1963. С. 333.

[2] Горбунов А.А., Кирьянов К.Г. // Вестник Нижегородского университета им. Н.И. Лобачевского. Серия Радиофизика. Н. Новгород: Изд-во ННГУ, 2005. Вып. 1(3). С.184.

[3] Кирьянов К.Г. // Труды V Межд. конф. «Идентификация систем и задачи управления SICPRO′05». М.: Изд-во ИПУ РАН, 2006. С.155.
[4] Горбунов А.А., Кирьянов К.Г. // Тр. 7-й Научн. конф. по радиофизике. Н.Новгород: ТАЛАМ, 2003. С.283.

ПРОГНОЗИРОВАНИЕ АНАЛОГОВЫХ И ДИСКРЕТНЫХ ПРОЦЕССОВ НА ОСНОВЕ ИДЕНТИФИКАЦИИ ИХ БАЗОВЫХ ПАРАМЕТРОВ

К.Г. Кирьянов[1)], Е.С. Кузнецов[2)]

[1)]*Нижегородский госуниверситет*
[2)]*Нижегородский государственный технический университет*

Идентификация и прогнозирование временных рядов (выборок из аналоговых непрерывных и разрывных процессов) применимы во многих практически важных случаях (в задачах анализа данных, в криптографии, задачах восстановления пропущенных в результате сбоев наблюдений и т.д.). Прогнозирование предлагаемым методом выполняется на основе оптимальных базовых параметров (БП): q (числа уровней квантования выборок ряда данных (2)), Δt (шага квантования по времени выборок данных (2)) и n (числа аргументов так называемого "прогнозирующего оператора" (ПО) для ряда (2)) (см., например, [1], [2]) – по единому новому энтропийному критерию:

$$E = -n \cdot \sum_{i=0}^{q-1} p_i \cdot \log_2 p_i \ , \qquad (1)$$

где p_i – оценка вероятности появления в тексте значения q_i, а не по известным зависимым от одного БП критериям оптимальности: отдельно для БП n и БП Δt – по критериям, например, H.Akaike (только для n) и В.А. Котельникова (только для Δt).

Идентификация основана на предварительном преобразовании исходных временных рядов в q-уровневые ряды длиной M:

$$\{y_k\}, k = 1,2,...,M < \infty \qquad (2)$$

путём определения их оптимальных БП.

Определение оптимальных базовых параметров заключается в нахождении такой тройки $\Delta t,q,n$ при которой у временного ряда (2) будет минимальная энтропия (1). Причём $T/M_{max} \le \Delta t \le T/M_{min}$ (где T – длительность исходного процесса), а $q_{min} \le q \le q_{max}$. Порядок прогнозирующего оператора определяется как минимальное n, при котором по одной и той же "n-ке" отсчетов (y_{k-n+1}, y_{k-n+2}, … , y_k) прогнозируются одинаковые значения $y_{k+1} = f_k$. Если изначально дан дискретный сигнал с заданной Δt, то определяются только q_{opt} и n_{opt}.

Если изначально имеется выборка из непрерывного сигнала с заданным Δt, то по имеющимся M отсчетам сигнал восстанавливается любым из известных методов, например В-сплайном Шенберга [4]. Затем для восстановленного (непрерывного) сигнала отыскивается оптимальная тройка $\Delta t_{opt}, q_{opt}, n_{opt}$.

Затем по ряду (2) строится ПО для любого $k=n,n+1, \ldots, M-1$ в виде q-значной логической функции с оптимальными БП

$$y_{k+1} = f(y_{k-n+1}, y_{k-n+2}, \ldots, y_k) \equiv f_k \qquad (3)$$

или эквивалентной таблицы истинности (ТИ). Строки ТИ ПО строятся по всем идущим подряд n членам ряда отсчетов ("n-кам" отсчетов) и следующему за ними отсчету, в качестве прогнозируемого ими символа.

Для придания «гибкой структуры» прогнозированию модифицируем функцию (3). Прогнозирование заключается в пошаговом построении продолжения ТИ с $M-n+1$-й по $M+sf$-ю строку, где $sf = 1,\ldots,Lf$, а Lf – номер максимального шага прогнозирования или т.н. «прогнозного горизонта» для пополнения выборок данных (2), имеющихся в исходной ТИ. Для определения $y_{M+sf} = f_{M+sf-1}$ используется последовательное сравнение y_{M-n+sf}-ой "n-ки" ($y_{M-n+sf}, y_{M-n+sf+1}, \ldots, y_{M+sf-1}$) со всеми "$n$-ми", уже имеющимися в исходной таблице, рассматриваемыми как опорные («эталонные») по критерию «минимума расстояния» между "n-ми" [3].

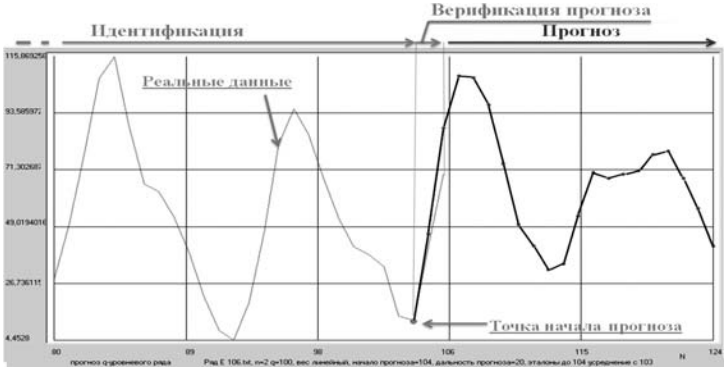

Рис.

На рисунке изображен пример прогноза для ряда солнечных пятен, взятого за 100 лет. У него были найдены q_{opt}=100, n_{opt}=2, Δt_{opt}=0.94 г. Жирной линией изображен ряд прогнозных значений. Тонкой – реальные данные. При верификации была подсчитана средняя относительная ошибка прогноза, равная 4,5%.

[1] Кирьянов К.Г. // Труды III Межд. конф. «Идентификация систем и задачи управления SICPRO′05». М.: Изд-во ИПУ РАН, 2004. С.187.
[2] Кирьянов К.Г., Горбунов А.А. // Информационные системы и технологии (ИСТ-2005): Тез. докл. Н.Новгород: НГТУ, 2005. С.158.
[3] Кирьянов К.Г., Кузнецов Е.С. // Информационные системы и технологии (ИСТ-2007): Тез. докл. Н.Новгород: НГТУ, 2007.С.154.
[4] http://art.vinnica.ua/rom/smg/144.htm

К АВТОМАТИЗАЦИИ ОБРАБОТКИ ДВУМЕРНЫХ ИЗОБРАЖЕНИЙ В РЕВМАТОЛОГИИ

Е.А. Грунина [1], К.Г. Кирьянов[2]

[1]*Нижегородская медицинская академия*
[2]*Нижегородский госуниверситет*

Ревматоидный артрит (РА) – это воспалительное ревматическое заболевание неизвестной этиологии, характеризующееся симметричным хроническим эрозивным артритом периферических суставов и системным воспалительным поражением внутренних органов [1]. РА течет с постоянно изменяющейся активностью воспаления и функцией суставов, тогда как повреждение суставов (костно-хрящевая деструкция) обычно постоянно прогрессирует. В настоящее время появились новые технологии лечения артрита, способные повлиять на скорость повреждения суставов и в ряде случаев затормозить или даже повернуть вспять этот процесс. В связи с этим особенно актуальными стали разработка и автоматизация методов диагностики и количественной оценки степени костно-суставной деструкции. Оптимальным в настоящее время по соотношению цена/информативность является рентгенографический метод с определением выраженности костно-суставной деструкции по Ларсену и Шарпу в модификации Ван дер Хайде [2].

До сих пор оценка рентгенограмм проводится врачом вручную.

К настоящему времени в мире разработаны четыре различных метода измерения ширины суставной щели с помощью компьютера и проведена их сравнительная оценка [3]. При этом авторы затруднялись измерять ширину щели в суставах запястья, а также во всех суставах при поздних стадиях артрита.

В настоящее время проблемы автоматизации рентгенологической оценки суставной деструкции связаны со сложностями на ряде этапов:

1) Автоматического выделения набора суставов для оценки.
2) Оценки ширины и площади суставной щели.
3) Обнаружения эрозий (краевых дефектов) кости.
4) Оценки площади эрозий.

Оценка количества и площади эрозий включает моделирование 3D-изображения, обводку «переднего» края эрозий, определение отсутствующего контура кости, измерение количества и площади эрозий. Начало работы по автоматизации оценки костно-суставной деструкции проведено студентами ННГУ и магистрантами НГТУ под руководством профессора К.Г. Кирьянова.

С помощью цифрового фотоаппарата рентгеновский снимок переводится в цифровой. Далее работа идет с пиксельной картой или массивом, в программе снимок предварительно переводился в режим “оттенки серого 8 разрядов”. Измерение линейных размеров происходит путём наложения электронной линейки поверх пиксельной карты рентгенограммы. Измерение площади поверхности проводится наложением измеряющейся площади поверх той, которую нужно измерить. Также есть возможность измерения объема эрозий. Диагностику эрозий проводит врач-оператор. В программе предусмотрен анализ неровностей области сустава, что де-

лает возможным после набора статистики полуавтоматический анализ состояния сустава. Полуавтоматический, потому что возможна такая стадия, на которой неровности на поверхности сустава уже не имеют такого значения. Последнее должен определить снова врач. Протоколирование: врач при работе с программой сделает пометки в виде текста. Далее эти пометки сохранятся отдельным файлом. Множество таких файлов составят базу данных для дальнейшей работы с полученной информацией.

При исследовании информативных параметров рентгеновских снимков выяснилось, что обнаружение числовых характеристик костно-суставной деструкции удобно проводить автоматизированно, если ввести новые информативные параметры выбранных врачом 2D-контуров с пораженными краями костей и щелей на пиксельной сетке рентгеновского снимка. Для этого по выбранным заданным параметрически координатам контуров $x=x(n)$, $y=y(n)$ строятся без потери упомянутой выше по п.п. 2)–4) нужной информации 1D-графики изменения кривизны $K(n)$ [4] по точкам $n=0,1,2,...,L$ вдоль выделенных линий или контуров

$$K(n)=\begin{vmatrix} x'(n) & y'(n) \\ x''(n) & y''(n) \end{vmatrix} \Big/ [(x'(n))^2+(y'(n))^2]^{3/2}, \qquad (1)$$

где производные аппроксимируются разностями координат на сетке снимка

$$x'(n)=x(n+1)-x(n),\ x''(n)=[x(n+2)-2x(n+1)+x(n)],\ y'(n),... , \qquad (2)$$

а 1D-графики $K(n)$ отображаются в т.н. базовые параметры (БП) любых выделенных врачом 2D-контуров и областей по формулам, приведённым в работе [5]. При этом, например, одним из БП является длина L графика $K(n)$, характеризующая длину 2D-линий или 2D-контуров.

При решении этого ряда задач разработка информационной автоматизированной системы выйдет за рамки оценки костно-суставной деструкции и станет возможной дифференциальная диагностика РА и ряда других суставных заболеваний.

[1] Насонова В.А., Насонов Е.Л., Алекперов Р.Т. и др. Рациональная фармакотерапия ревматических заболеваний: Рук. для практикующих врачей / Ред. В.А. Насонова, Е.Л. Насонов. М.: Литтерра, 2003. С.87.
[2] Ory P.A. // Ann. Rheumatol. Dis. 2003. V.62. P.597.
[3] Sharp J.T., Angwin J., Boers M. et al. // J. Rheumatol. 2007. V. 34, No.4. P.874.
[4] Бронштейн И.Н., Семендяев К.А. Справочник по математике. М.: ГИТТЛ , 1953. С.240.
[5] Кирьянов К.Г. // Труды III Межд. конф. «Идентификация систем и задачи управления SICPRO′04». М.: Изд-во ИПУ РАН, 2004. С.187.

ПЛАНИРОВАНИЕ ГОЛОСОВОГО ТРАФИКА С ПОДДЕРЖКОЙ QoS

А.В. Малыгин, Л.Ю. Ротков

Нижегородский госуниверситет

В мире современной телефонии происходит постепенный переход от традиционных телефонных сетей общего пользования (ТфОП) к сетям с пакетной коммутацией. Причина этого в том, что Интернет-телефония дает снижение стоимости переговоров в несколько раз, что особенно важно для дорогих междугородних и межнациональных соединений. Однако существующие IP-сети еще не способны адекватно обеспечивать передачу голоса поверх Интернет-протокола (VoIP). Со стороны сети требуется развитая поддержка качества обслуживания (QoS). На протяжении всего виртуального канала между собеседниками в каждой точке, где потенциально возможен дефицит ресурса (например, пропускной способности канала), должны функционировать QoS-механизмы.

Одними из подобных мест, «узких» с точки зрения поддержания качества обслуживания, являются планировщики пакетов на маршрутизаторах. Обеспечивая справедливое распределение пропускной способности выходящего канала между несколькими потоками, планировщик, как правило, не следит за соблюдением требований голосового трафика – ограничения задержки пакетов и минимизации джиттера и потерь пакетов из-за переполнения буфера. Кроме этого, вычислительная простота планировщика достигается ценой отсутствия изоляции потоков VoIP друг от друга.

Сейчас на маршрутизаторах Cisco применяются несколько схем планирования пакетов: WFQ (Weighed Fair Queueing), WF^2Q (Worst-case Fair WFQ), P-WFQ (Priority-based WFQ), PQ/WFQ (Priority Queue/ WFQ) и LLQ (Low Latency Queueing) [1]. Эти планировщики наряду с потоками обычных данных призваны обслуживать и потоки VoIP. Применительно к обслуживанию голосового трафика каждая схема планирования имеет определенные недостатки.

В WFQ с каждым поступающим пакетом связывается тег, который представляет собой виртуальное время окончания передачи этого пакета при использовании идеализированной схемы GPS (Generalized Processor Sharing). В GPS все активные потоки обслуживаются одновременно. Согласно WFQ, пакеты передаются в выходной канал в порядке увеличения значений их тегов. В WFQ гарантируется отсутствие отставания относительно GPS в обслуживании потока с начала периода занятости сервера ($t = 0$) более чем на размер максимального пакета в системе:

$$G_i(0;t) - S_i^{WFQ}(0;t) \le L_{max}, \qquad (1)$$

где $G_i(0;t)$ и $S_i^{WFQ}(0;t)$ – трафик i-го потока, обслуженный в интервале времени $(0;t)$ при GPS и WFQ соответственно; L_{max} – максимальный размер пакета в системе.

Однако при этом не ограничивается возможное опережение WFQ в обслуживании i-го потока:

$$\exists c \geq 0 : \; S_i^{WFQ}(0;t) - G_i(0;t) \leq cL_{max} . \qquad (2)$$

Проблема неограниченного джиттера задержки, свойственная WFQ, была преодолена в схеме WF^2Q введением условия «избираемости» пакетов для планирования. Только те из пакетов, которые уже начали передаваться в GPS, становились кандидатами на планирование в WF^2Q. В результате было ограничено опережение в обслуживании потоков относительно GPS, а вместе с этим и джиттер задержки:

$$S_i^{WFQ}(0;t) - G_i(0;t) \leq \left(1 - \frac{r_i}{r}\right) L_i^{max} , \qquad (3)$$

где r – пропускная способность (ПС) канала; r_i – минимальная ПС, гарантированная i-му потоку при GPS и определяемая следующим образом:

$$r_i = \frac{\omega_i}{\sum_{j=1}^{N} \omega_j} r , \qquad (4)$$

где ω_i – весовой коэффициент i-го потока; N – количество активных потоков.

Из (3) и (4) следует, что понизить джиттер VoIP-пакетов можно путем увеличения зарезервированной за голосовым трафиком ПС канала. Это влечет за собой неэффективное использование канала, что неприемлемо.

P-WFQ решает последнюю проблему путем назначения низкоскоростным VoIP-потокам наивысшего приоритета и введения механизма скользящего окна. Однако уменьшение задержки VoIP-пакетов достигается ценой снижения справедливости разделения ПС канала. Кроме этого, возникает проблема джиттера VoIP-пакета, еще не попавшего в скользящее окно, на величину, равную времени передачи максимального пакета в системе.

В схемах PQ/WFQ и LLQ VoIP-пакеты направляются в специальную приоритетную очередь. Остальные потоки обслуживаются согласно WFQ и Class-based WFQ соответственно. Наличие только одной приоритетной очереди ведет к проблеме отсутствия изоляции VoIP-потоков друг от друга, что, в итоге, снижает QoS.

Таким образом, проблема планирования голосового трафика с поддержкой QoS на данный момент остается без решения.

[1] Chen X., Wang C., Xuan D., Li Z., Min Y. and Zhao W. Survey on QoS Management of VoIP // Proc. 2003 Int. Conf. on Computer Networks and Mobile Computing (ICCNMC'03), 2003.