ИНФОРМАЦИОННЫЕ СИСТЕМЫ

СРЕДСТВА, ТЕХНОЛОГИИ, БЕЗОПАСНОСТЬ

ИЗМЕНЕНИЕ ПАРАМЕТРОВ ЗАДЕРЖЕК СООБЩЕНИЙ В СЕТЯХ СОТОВОЙ СВЯЗИ

Е.С.Золотницкий, Л.Ю.Ротков

Нижегородский госуниверситет

Проблема эха в системах связи известна ещё с момента появления аналоговой телефонии. Абоненты телефонных сетей при разговорах на больших расстояниях (например, при межконтинентальных соединениях) столкнулись с неприятным эффектом: из-за задержки в распространении сигнала помимо голоса собеседника в телефоне слышен собственный голос, задержанный на некоторое время. Этот эффект затрудняет комфортное общение, а иногда делает его невозможным. Причина возникновения данного типа эха – несогласованность импедансов двух проводной и четырёх проводной линий в преобразователе 2–4-проводную линию.

Эффект эха усиливается при значительной задержке распространения сигнала. Так, в [1] показано, что эхо с задержкой более 36 мс ухудшает разборчивость и слышимость речи или музыки.

Устранение нежелательного эха осуществляют двумя методами: эхо подавлением и эхо компенсацией. Подавитель – это простая пара активируемых голосом переключателей, которые сокращают эхо производя затухание в обратном пути передачи четырёх проводной магистральной линии [2], [3]. Компенсатор – это цифровое устройство, генерирующее реплику эха, используя адаптивный алгоритм, и вычитающее её из сигнала.

В современных сетях сотовой телефонии второго поколения (GSM/DCS, IS-95 CDMA, IS-136 TDMA) также остро стоит проблема эха. Так, эффект эха усиливается за счёт дополнительных задержек, вносимых цифровыми элементами таких сетей. Это задержки в ЦАП, АЦП, кодерах речи и канала, а также задержки, возникающие в наземной инфраструктуре сети: при мультиплексировании, цифровой интерполяции, прохождении сигнала через контроллеры и коммутаторы.

Задержка в распространении сигнала становится меняющейся по времени в процессе одного вызова из-за переменной скорости движения подвижной станции, хендоверов, задержек сигнала в очередях, пакетизации, потери кадров/ячеек при транспортировке, компрессии/декомпрессии речи, разнице в тактовых частотах не синхронизированных компонентов сети. В результате компенсатор не успе-

вает перестроиться (сойтись) к новому значению задержки и нежелательное эхо компенсируется не полностью.

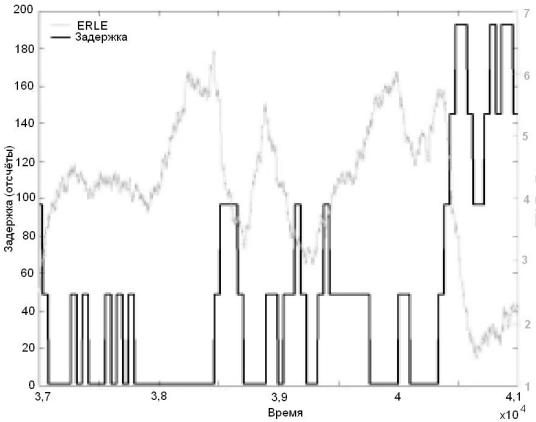
В рекомендациях ITU-T G.165, G.168 определены основные параметры эхо компенсаторов. Это время сходимости (время разработки модели пути эха, остаточный уровень эха д.б. на 27 дБ ниже уровня сигнала) и увеличение затухания обратного эха (ERLE – Echo Return Loss Enhancement).

$$ERLE = 10 \lg \frac{P_{сэ}}{P_{оэ}}, \tag{1}$$

где $P_{сэ}$ – мощность сигнала эха, а P – мощность сигнала остаточного эха.

Для стационарных сигналов выражение для *ERLE* принимает следующий вид:

$$ERLE = 10 \lg \frac{\sum_{i=0}^{N_1-1} w_i^2}{\sum_{i=N}^{N_1-1} w_i^2}, \tag{2}$$



где N_1 – длина дискретной версии импульсного отклика, порождающего эхо сигнал, N – длина адаптивного фильтра, w_i – коэффициенты импульсного отклика адаптивного фильтра.

На рис. показано изменение *ERLE* в зависимости от изменения величины задержки.

Работа выполнена при поддержке гранта Федерального агентства по образованию № А04-2.9-1099.

[1] Анерт В., Райхардт В. Основы техники звукоусиления. — пер. с нем. п/р Белкина Б.Г. — М.: Радио и связь, 1984. — 320 с.

[2] Stephen B. Weinstein, '*Echo Cancellation in the Telephone Network*', IEEE Communications Society Magazine, January 1977.
[3] Man Mohan Sondhi, David A. Berkley, '*Silencing Echoes on the Telephone Network*', Proceedings of the IEEE, Vol. 68, No. 8, pp. 948–963, August 1980.

ВОЗМОЖНОСТИ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ МЕХАНИЗМА TDM В НАЗЕМНОЙ ИНФРАСТРУКТУРЕ СЕТИ GSM

Е.С.Золотницкий, А.В.Малыгин

Нижегородский госуниверситет

В настоящее время сотовая телефония представляет собой одну из наиболее быстро развивающихся отраслей в сфере высоких технологий. Постоянно растущие потребности в передаче различного рода трафика (речь, данные, мультимедиа) обнажают недостатки наземной инфраструктуры сетей сотовой связи второго поколения. Одним из таких изъянов является неэффективное использование полосы битовой скорости передачи потока E1. Согласно механизму временного разделения канала (Time Division Multiplexing, TDM), применяемому в наземной инфраструктуре сетей GSM, за каждым абонентом в течение сеанса связи закрепляется целый временной слот потока E1, который уже не может использоваться для передачи сжатой речи других абонентов, когда первый молчит. В данной работе рассматривается применение технологии трансляции кадров Frame Relay к передаче сжатой речи на участке сети между контроллером базовых станций (Base Station Controller, BSC) и транскодером (Transcoder, TC), как на одном из участков высокой концентрации трафика.

Исследования, проведенные в XX веке научно-исследовательскими лабораториями телефонных компаний (например, Bell Labs [1]), показали, что отрезки абонентской речи (сегменты речи) обладают следующими закономерностями:

1) длительности сегментов подчиняются отрицательному экспоненциальному распределению со средним значением $t_{sp} = 300$ мс;
2) моменты поступления речевых сегментов в сеть подчиняются пуассоновскому распределению;
3) средняя интенсивность нагрузки, создаваемая абонентом, составляет $\rho = 0{,}4$ Эрл.

Любой BSC обеспечивает передачу сжатой речи к TC посредством A-trunk интерфейса (см. рис.1). DTC (Digital Trunk Controller) – магистральный контроллер, обеспечивающий передачу сжатой речи по тридцати 16-килобитным каналам и сигнальной информации – по линии SS№7. Повышение использования полосы передачи потока E1 требует рассмотрения DTC как системы массового обслуживания, имеющей 30 приборов и конечную очередь на обслуживание.

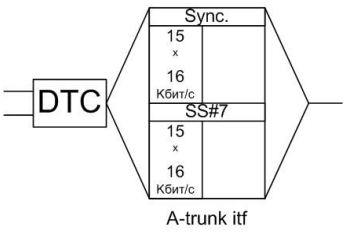


Рис. 1

С учетом механизма прерывистой передачи речи средняя интенсивность нагрузки, создаваемая одним вызовов, определяется выражением, представленным формулой (1):

$$\rho_{eff} = \rho_{sp}\frac{t_f}{t_{sp}} + (1-\rho_{sp})\frac{1}{T_{sp}}(T+\frac{h}{c}) \cong 0{,}46\,, \qquad (1)$$

где: $t_f \approx$ 323 мс – среднее время обслуживания одного кадра Frame Relay, несущего один речевой сегмент или его часть, если он состоит более, чем из 51 кадра сжатой речи (с учетом SID-кадра (Silence Descriptor Frame), следующего за каждым речевым сегментом);

T_{sp} = 0,5 с – период следования SID-кадров в интервале молчания абонента;

T = 20 мс – длительность одного кадра сжатой речи в соответствии со стандартом GSM;

h = 48 бит – длина заголовка кадра Frame Relay (вместе с CRC и флагами);

c = 16 Кбит/с – пропускная способность одного канала передачи сжатой речи.

Табл.

Показатель QoS	Значение
B	≤ 0.001
Mξ	≤ 20 мс
σ(ξ)	≤ 20 мс

Заменяя полученный составной трафик сегментов сжатой речи и SID-кадров, упакованных в кадры FR, эквивалентным по предлагаемой нагрузке трафиком, но имеющим отрицательное экспоненциальное распределение длительности обслуживания со средним значением t_f, можно получить заниженное, но гарантированное количество вызовов, поддерживаемых одним DTC. В итоге DTC можно анализировать как модель многоканальной СМО с конечной очередью *M/M/N/L*, где N = 30.

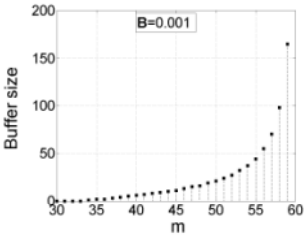


Рис. 2

Максимально возможное количество вызовов, поддерживаемых одним DTC при таком использовании технологии Frame Relay, определяется условиями, накладываемыми на показатели качества обслуживания (Quality of Service, QoS) (см. таб.): вероятность потери сегмента **B** (переполнение очереди), среднее время задержки сегмента в очереди **M**ξ (при его попадании в нее), джиттер этой задержки **σ**(ξ) (с.к.о.). На рис. 2 представлена зависимость требуемого размера очереди L в зависимости от количества поддерживаемых одним DTC вызовов m. На основании этой зависимости получены зависимости **σ**(ξ) и **M**ξ при **B** ≈ 0,001**,** представленные на рис.3. Из рис.3 следует, что максимально возможное гарантированное количество вызовов, которое способен обслуживать один магистральный контроллер при обеспечении QoS (см. таб.), составляет 46. В

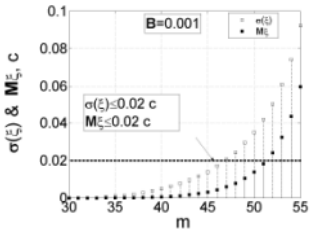


Рис. 3

итоге достигнуто повышение использования полосы битовой скорости передачи потока E1 более чем в 1,5 раза.

Работа выполнена при поддержке гранта Федерального агентства по образованию № А04-2.9-1099.

[1] Technical Staff, Bell Telephone Laboratories, Engineering and Operations in the System, Western Electric, Indianapolis, 1977.

ИССЛЕДОВАНИЕ КЛИППИРОВАНИЯ В ЧАСЫ НАИБОЛЬШЕЙ НАГРУЗКИ НА УЗЛАХ КОММУТАЦИИ МЕЖДУГОРОДНИХ АТС

Е.С.Золотницкий, А.В.Малыгин

Нижегородский госуниверситет

Клиппирование или обрезание фрагментов речи представляет собой одну из неизбежных проблем современной телефонии общего пользования (ТфОП). Причин тому несколько: эхо подавители, способные работать лишь в полудуплексном режиме; превышение шумом определенного порога или недостаточное отношение уровня сигнала к уровню шума; задержка коммутации и нехватка выходных каналов на междугородних автоматических телефонных станциях (АТС). Современный уровень развития высоких технологий позволяет сравнительно недорого решить две первые проблемы переходом к интеллектуальным устройствам – эхокомпенсаторам и цифровой передаче соответственно. Задержка коммутации останется по причине дороговизны неблокируемых коммутационных матриц. Проблема нехватки выходных каналов по экономическим соображением разрешима лишь до уровня предоставления абонентам определенного гарантированного качества обслуживания (Quality of Service, QoS). Количество выходных линий должно быть рассчитано на активность абонентов в час наибольшей нагрузки (ЧНН). Наиболее выгодное решение этой проблемы заключается в применении систем интерполяции речи с временным разделением (Time Assignment Speech Interpolation, TASI), когда конкретный абонент подключается к какому-либо доступному каналу из пучка линий лишь при наличии активности. Системы TASI также широко применяются в сельской местности при обеспечении доступа абонентов к меньшему числу каналов.

В терминологии теории массового обслуживания система TASI является системой с удержанием заблокированных вызовов и конечным числом источников. Нагрузка поступает от M источников и обслуживается N ($N < M$) каналами-приборами. Применительно к речевому трафику, характеризующемуся пуассоновским распределением моментов поступления и отрицательным экспоненциальным распределением длительности речевых сегментов, вероятность удержания отрезка (сегмента) речи определяется формулой (1) [1]:

$$B_h = \sum_{n=N}^{M-1} C_{M-1}^{n} \rho^n (1-\rho)^{M-1-n} \qquad (1)$$

где $\rho = 0{,}4$ – нагрузка одного канала в ЧНН.

Важным показателем QoS является доля клиппированной нагрузки. Она определяется как отношение интенсивности непереданной нагрузки к поступающей интенсивности нагрузки [2]:

$$B_{клип} = \frac{1}{M\rho} \sum_{n=N+1}^{M} (n-N) C_M^n \rho^n (1-\rho)^{M-n} \qquad (2)$$

Средняя величина вырезок среди клиппированных сегментов определяется как отношение доли клиппированной нагрузки к вероятности клиппирования:

$$B^*_{клип} = B_{клип} / B_h \qquad (3)$$

Формула (2) для непосредственного использования не годится, так как реально количество каналов, поддерживаемых одной междугородной АТС, может достигать двух сотен тысяч. С помощью интегральной теоремы Муавра-Лапласа было получено приближенное выражение для $B_{клип}$:

$$B_{клип} = \frac{1-\rho}{M}\left(\frac{\partial z}{\partial \rho} - \frac{N-M\rho}{\rho(1-\rho)} z\right) \qquad (4)$$

где:

$$z = \frac{1}{2}\left[\operatorname{erf}\left(\sqrt{\frac{M(1-\rho)}{2\rho}}\right) - \operatorname{erf}\left(\frac{N+1-M\rho}{\sqrt{2M\rho(1-\rho)}}\right)\right] \qquad (5)$$

и *erf*(*x*) – функция ошибки, равная:

$$\operatorname{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-z^2} dz \qquad (6)$$

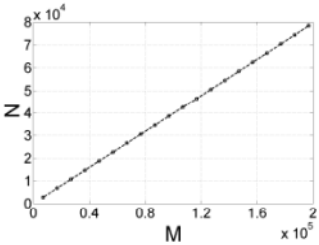


Рис. 1

Рекомендацией ITU-T E.855 определен максимально допустимый порог для величины потерянной нагрузки – 0,5%. График на рис.1 иллюстрирует минимальное количество каналов *N*, необходимое для обслуживания *M* вызовов. При больших *M* (*M*>1000) зависимость *N*(*M*) линейна с коэффициентом ρ = 0,4. На рис.2 представлен график зависимости величины вырезок в клиппированных речевых сегментах от количества входящих вызовов, на которые рассчитана АТС. Из графика следует, что чем на большее число вызовов рассчитана данная АТС, тем меньшее влияние клиппирования ощущается абонентами в ЧНН. Можно сделать вывод о том, что наибольшие неудобства клиппирование доставляет пользователям небольших районных АТС, рассчитанных на несколько сотен абонентов и использующих механизм TASI.

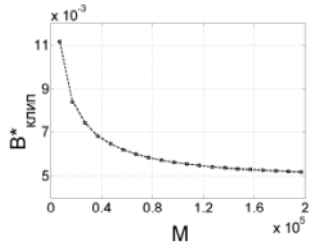


Рис. 2

Работа выполнена при поддержке гранта Федерального агентства по образованию № А04-2.9-1099.

[1] Беллами Дж. Цифровая телефония: Пер. с англ. /Под ред. А.Н. Берлина, Ю.Н. Чернышева.- М.: Эко-Трендз, 2004.-640 с., илл.
[2] C.J. Weinstein, «Fractional Loss and Talker Activity for Switched Speech», IEEE Transactions on Communications Technology, Aug. 1978, pp. 1253-1256.

СИСТЕМА МОНИТОРИНГА СОСТОЯНИЯ РАБОТ НА ОСНОВЕ WEB-ТЕХНОЛОГИЙ

С.Л.Моругин, М.В.Ширяев

Нижегородский государственный технический университет

Цель разработки системы – повышение качества управления учебными заведениями через улучшение информационного обмена, повышение надежности информационного обмена между Департаментом образования РФ и органами исполнительной власти, органами управления образованием, органами управления по делам молодежи субъектов РФ, учебными заведениями высшего и среднего профессионального образования путем разработки и внедрения автоматизированных рабочих мест.

Обеспечение информационного обмена включает массовую рассылку информационных сообщений и документов, а также мониторинг состояния работ

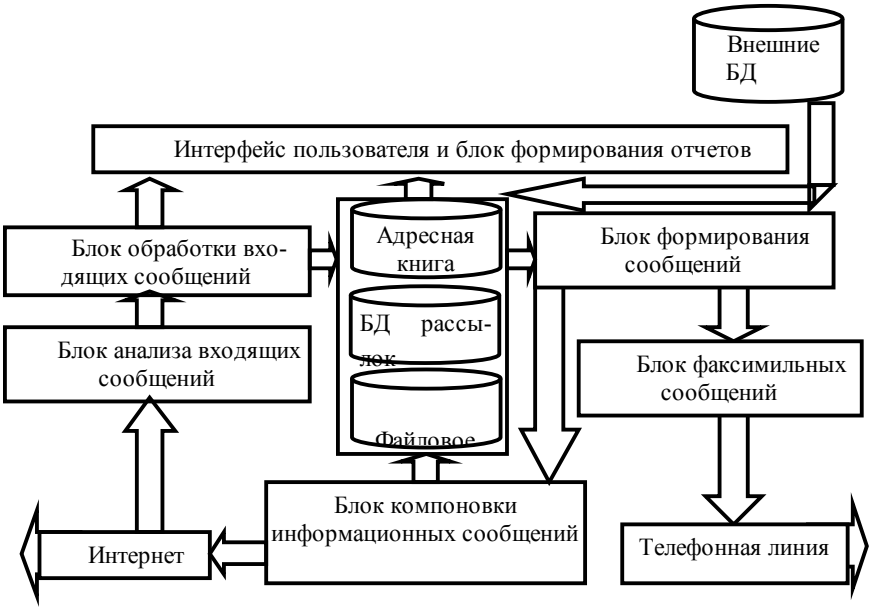
Отделы и подразделения Департамента образования РФ формируют нормативные и прочие документы, подлежащие рассылке. Они определяют, кому эти документы предназначены. Эти сведения передаются в отдел рассылок, который непосредственно занимается отправкой информационных сообщений.

АРМ позволяет решить следующие задачи:

- обеспечение автоматического выставления на сайт почты для заданного числа абонентов;
- автоматический ввод информации об адресах получателей из баз данных;
- разделение входящих и исходящих информационных сообщений по категориям доступа и получателям;
- автоматизация переписки с организациями и учреждениями;
- обработка результатов доставки сообщений (подтверждение доставки, ведение протокола доставки);

Документы в отдел могут приходить как в бумажном, так и в электронном виде. Бумажные документы приводятся к электронному виду. Далее формируется информационное сообщение и осуществляется рассылка.

Вся информация о рассылке автоматически фиксируется в базе данных. Если в процессе рассылки возникли исключения (ошибки при осуществлении информационного обмена), то автоматически их обрабатывает подсистема анализа результатов рассылки, с уведомлением пользователя и составлением отчета.



Публикация баз данных средствами web-технологий позволяет вместо рассылки сообщений делать их доступными для вузов при просмотре через web-интерфейс. Это сокращает время на рассылку сообщений, делает более четкой работу системы мониторинга доставки и прочтения.

Мониторинг выполнения работ позволяет:

- автоматизировано отслеживать состояние работ, выполняемых вузами (по целевым программам, заказ нарядам, учебной работе и др.).
- автоматически посылать в адрес вуза сообщения и извещения при нарушении регламентируемых временных и количественных показателей, отслеживаемых системой мониторинга;
- получать сводные данные по множеству подконтрольных вузов и других учебных заведений по таким вопросам, как:
    - предоставление отчетов и документов к заданному сроку;
    - достижение контрольных показателей к заданному сроку;
    - нарушение допустимой степени отклонения контрольных показателей;
- организовать автоматизированный сбор данных по множеству программируемых показателей путем заполнения вузами форм сбора данных;
- автоматизировать обработку массивов собранных данных с получением статистических показателей.

Применение разрабатываемой системы позволит существенно сократить затраты времени на рассылку сообщений, сбор и обработку данных, мониторинг состояния различных видов работ.

АЛГОРИТМ «МЯГКОГО» РАСПРЕДЕЛЕНИЯ ПРАВ ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ РЕСУРСАМ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Д.В.Прохоров, В.П.Хранилов

Нижегородский государственный технический университет

Обеспечение безопасности и защиты информации является актуальной проблемой при использовании современных информационных технологий. Потребительские свойства и удобство специализированных подсистем авторизации и разграничения доступа в современных вычислительных сетях (ВС) далеки от совершенства. Процессы разграничения доступа к системе разных категорий пользователей и опытная эксплуатация ВС, как правило, разделены функционально и во времени, что создает дополнительные затруднения и замедление сроков внедрения ВС.

Предлагается новый алгоритм разграничения прав доступа пользователей к информационным ресурсам ВС, построенный в интерактивном режиме на основе процедуры распределения ресурса безопасности отдельных программных модулей, с учетом потенциальных характеристик безопасности пользователей и параметров требуемой защищенности модулей.

Решение задачи разграничения доступа пользователей к ВС требует выполнения взаимосвязанных действий, связи между которыми описываются с помощью операции отображения **Г: M→Q** [1] исходного проблемно-ориентированного набора (ПОН) программных модулей – множества **M** в множество **Q,** представляющее собой совокупность объектно-ориентированных наборов (ООН), соответствующих требованиям и ограничениям по информационной безопасности (ИБ). Будем считать, что принятие решений, связанных с формированием системы ООН программных модулей на рабочих станциях ВС с заданными требованиям по ИБ, аналогично распределению ресурсов ИБ программных модулей с учетом характеристик потенциальной ИБ пользователей и параметров защищенности модулей.

Цель процесса распределения ресурсов – гибкое адаптивное разграничение прав доступа пользователей к программным модулям ПОН путем выполнения в интерактивном режиме заданного комплекса взаимосвязанных работ таким образом, чтобы при заданных характеристиках ресурсов ИБ модулей и потенциала ИБ пользователей оптимизировать выбранную целевую функцию, выражающую меру эффективности [2,3] системы ИБ.

Разграничение прав доступа предполагается реализовать в интерактивном режиме, поэтому целесообразно выделить в процедуре формирования ООН фазу принятия решения с включением m_i в промежуточный набор **V** и фазу непосредственной сборки m_i в ООН **Q**. Следовательно, основное отображение разбивается на

два уровня: $\mathbf{\Gamma_1: M \to V}$ и $\mathbf{\Gamma_2: V \to Q}$, где **V** – множество пробных наборов, имитирующих процесс формирования ООН.

Доказывается [4], что универсальным математическим аппаратом для адекватного формального описания поставленной задачи является аппарат нечетких множеств (НМ). Состояние элементов формируемой системы $m_i \in \mathbf{M}$ может быть описано НМ **A**, заданным на базовом множестве **Q** и образованным прямым отображением $\mathbf{\Gamma: M \to Q}$. При этом $\mathbf{A}(m_i)=\{<\mu(m_i),\mathbf{Q}>\}=\{\mu(m_i)/\mathbf{Q_1};\mu(m_i)/\mathbf{Q_2};...\mu(m_i)/\mathbf{Q_j};$ $...\mu(m_i)/\mathbf{Q_m}\}$, где $\mu(m_i)$ – степень принадлежности m_i к ООН $\mathbf{Q_j}$; $n=|\mathbf{M}|$; $m=|\mathbf{Q}|$.

Вид применяемой модели [1] определяется характером решаемой задачи. В векторной форме: $\mathbf{Y=F(M,V,Q,P,\Lambda)}$, где **F** - теоретико-множественный функционал, выражающий соответствие $\boldsymbol{q}=\mathbf{(M \to V \to Q,P,Y,F)}$ с учетом воздействия внешних факторов $\mathbf{\Lambda}$. Вектор управляемых переменных – $\mathbf{P} = (p_1, p_2, \ldots p_n)$, выходные параметры – вектор $\mathbf{Y} = (y_1, y_2, \ldots y_m)$. Управляемые переменные **P** и выходные характеристики **Y** определяют свойства исследуемой системы, а внешние параметры $\mathbf{\Lambda}$ характеризуют внешнюю среду.

Параметры ИБ модулей и пользователей в принятой математической модели принадлежат к векторам управляемых переменных **P** и выходных характеристик **Y**. Идентифицируем параметры ИБ и компоненты векторов **P** и **Y** одного модуля $m_i \in \mathbf{M}$ для случая обращения к нему *j*-го пользователя при попытке сформировать маршрут $\mathbf{V}_i$: p_1 – параметр ИБ модуля (категория секретности) ; p_2 – параметр потенциала ИБ пользователя (форма допуска), p_3 – стаж работы пользователя; p_4 – индивидуальные характеристики пользователя, выражающие степень доверия работодателя (досье); $y_j = F(m_i,v_i,q_i,p_1,p_2,p_3,p_4,\lambda_1,\lambda_2,\lambda_3,\lambda_4)$. Входные параметры, формирующие функцию выходной характеристики y_j и определяющие текущее состояние модулей относительно формируемого ООН, используются для определения $\mu(m_i)$.

С использованием значений параметров формируются критерии «жесткого» и «мягкого» разрешения доступа к модулям, интегральные критерии ИБ системы, критерий риска и критерий эффективности защиты.

Относительная гибкость и адаптивность системы обеспечиваются: интерактивным режимом работы; адекватной структурой параметров ИБ, ориентированной на существующие законодательные нормы в области ИБ; применением специальных способов математической обработки этих параметров, обеспечивающих сопоставимость разнородных показателей; применением математического аппарата НМ.

Применение разработанных моделей и методов разграничения прав доступа пользователей, в отличие от используемых в современных ВС, позволяет проводить адаптацию системы информационной безопасности в интерактивном режиме без влияния на функционирование пользователей и без грубого вмешательства в их производственную деятельность.

[1] Хранилов В.П. //Известия АИН. 2004. Т. 9. С.19.

[2] Батищев Д.И., Коган Д.И. Вычислительная сложность экстремальных задач переборного типа.– Н.Новгород: ННГУ, 1994, 115 с.
[3] Батищев Д.И. Принятие оптимальных решений в экономических исследованиях.– Горький: ГГУ, 1982, 108 с.
[4] Хранилов В.П.//В кн.: Тр. научн. конф. SICPRO`03.– М: ИПУ РАН, 2003,С.1481.

АЛГОРИТМ ЗАЩИТЫ ОТ СЕТЕВЫХ АТАК ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»

А.А.Борисов, Л.Ю.Ротков, А.С.Ромашев

Нижегородский госуниверситет

На сегодняшний день уделяется большое внимание вопросам безопасности сетей, и способности сетевого оборудования противостоять атакам злоумышленников направленных на нарушение работоспособности сети и выведения из строя активного сетевого оборудования. В общем случае направления атаки можно разделить на 2 группы:

- каналы передачи данных;
- сервисы, предоставляемые сетью.

С атаками первого типа бороться практически невозможно. Можно увеличивать пропускную способность канала, но через некоторое время будет создано оборудование способное полностью заполнить полосу пропускания канала передачи данных.

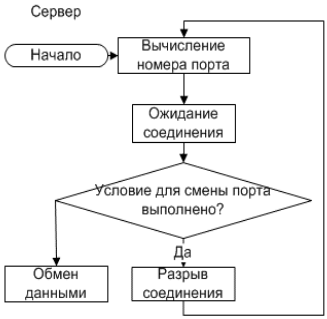
Для атак второго типа разработан ряд средств реализующих методы защиты, основанные либо на ограничении числа потенциальных клиентов, либо на установку мощного и дорогого оборудования межсетевых экранов, которые выполняют задачи фильтрации трафика по некоторым критериям, и в той или иной мере способны противостоять атакам злоумышленников. Но большинство этих способов становятся непригодными по отношению к атакам «отказа в обслуживании» (DOS). Атака DOS является легко реализуемой, и при этом, самой результативной. Простота реализации атаки связана с особенностью реализации большинства современных сервисов. Для своей работы они используют соответствующий стек протоколов (протокол транспортного уровня TCP или UDP и протокол сетевого уровня IP) и предоставляют услуги при неизменном номере порта. Увеличение интенсивности запросов на обслуживание сделает через определенное время сервис недоступным, так как вычислительные ресурсы сервера и систем защиты ограничены.

Решим проблему противостояния атакам отказа в обслуживании на стороне сервера. Пусть сервис, способен менять номер порта по некоторому закону

$$P(t) = f(a_1, a_2, \ldots a_n),$$

где $f(a_1, a_2, \ldots a_n)$ – функция нескольких переменных, например, таких как системное время, флаги наличия атак, обнаруженных сетевым оборудованием и других.

Алгоритм смены порта и работы сервиса изображен на рисунке. Изменение алгоритма работы серверного программного обеспечения требует соответствующего клиентского программного обеспечения, причем функция $f(a_1, a_2, \ldots a_n)$ должна быть известна клиенту.



Теоретически модель, описанная выше должна обладать большей устойчивостью к атакам отказа в обслуживании. Сравнение производительности стандартного ftp-сервера и разработанного сервера проведено экспериментально при передаче данных объемом 200 – 700 мегабайт. В результате эксперимента установлено, что при отсутствии атак разработанный сервер передает данные на 10 – 15 % медленнее по сравнению с обычным ftp-сервером. При проведении DOS атак ftp-сервер переставал функционировать, а сервер, построенный по предложенному алгоритму, продолжал работать, хотя на передачу данных тратилось больше времени, чем при отсутствии атак. На основании проведенных экспериментов подтверждено, что разработанный алгоритм обеспечивает достаточно высокую эффективность в противостоянии атакам отказа в обслуживании.

[1] Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации.– М.,1998. –245 с.
[2] Justin J. Lister. Latest Developments and New Technologies for Detecting and Preventing Computer, Communication and Financial Fraud.
[3] Лукацкий А.В. Системы обнаружения атак. –Банковские технологии, 2, 1999. с.54-58
[4] Баранов А.П. Обнаружение нарушителя на основе выявления аномалий ″Проблемы информационной безопасности″, 1, 1999. с. 44-50.
[5] Гэри Бернстайн. Мошенничество – в центре внимания. ″Mobile Communication International/RE″, 1, 1999. с. 28-30.
[6] RFC 793.

ПОСТРОЕНИЕ ПРИЗНАКОВОГО ПРОСТРАНСТВА КОМПЬЮТЕРНОЙ СИСТЕМЫ МЕТОДОМ КОРРЕЛЯЦИОННЫХ ПЛЕЯД

И.Б.Шинкаренко, Л.Ю.Ротков, С.В.Корелов

Нижегородский госуниверситет

Вопрос формирования признакового пространства (набор неких характеристик, отражающих свойства изучаемых объектов) является одним из ключевых в построении системы обнаружения вторжений в компьютерных системах (КС).

Признаковое пространство должно удовлетворять следующим требованиям:

- измеряемость (все признаки пространства должны быть доступны непосредственному измерению);
- информативность (признаки должны нести максимум полезной информации об объектах);
- минимально допустимая размерность (для уменьшения избыточности).

Формализованные методы формирования словаря первичных признаков не известны, поэтому при решении задачи необходимо опираться на ее характер и априорную информацию об объектах.

Под снижением размерности понимается формирование нового словаря, размерность которого меньше, а информативность сохранена максимально возможной. Признаки нового словаря могут быть либо первичными признаками, либо могут быть образованы из первичных по некому правилу (линейная комбинация, квадратичная функция и т.п.) Такие обобщенные признаки, заменяющие с достаточной точностью группы исходных признаков, называют факторами. Таким образом, на основе словаря первичных признаков проводится описание некого набора объектов, формируется статистика, и на основе этой статистики строятся факторы.

Все задачи снижения размерности можно разбить на два класса [1]:

1) Построение объясняющих факторов («глубинных», непосредственно не наблюдаемых признаков), которые объясняют изменение исходных признаков.
2) Построение представляющих факторов – факторов, наилучшим образом заменяющих группы исходных признаков.

Объясняющие факторы являются функциями первичных признаков и в общем случае непосредственно не измеряемы, что не отвечает выше оговоренным требованиям. Следовательно, для формирования признакового пространства КС имеет смысл использовать методы построения представляющих факторов.

Методы построения представляющих факторов основаны на гипотезе, что множество исходных признаков $\vec{\xi} = \{\xi_1 \ldots \xi_n\}$ естественно разделяется на такие группы, в каждой из которых изменения обусловлены в основном каким-

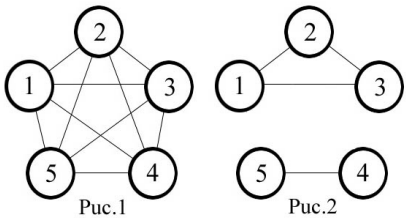


Рис.1

Рис.2

то одним общим фактором, а влияние этого общего фактора на другие группы признаков незначительно.

Для нахождения таких групп признаков можно использовать метод корреляционных плеяд [1]. Плеяды выбираются таким образом, чтобы внутренняя связь (корреляционная связь между признаками одной группы) была достаточно велика, а «межплеядная» (корреляционная связь между признаками разных групп) – мала.

Рассмотрим корреляционную матрицу $R=\|r_{ij}\|_{n\times n}$ первичных признаков, где:

$r_{ij}=\dfrac{\frac{1}{N}\sum_{k=1}^{N}\left(\xi_i^k-\bar{\xi}_i\right)\left(\xi_j^k-\bar{\xi}_j\right)}{\sqrt{D_i\cdot D_j}}$ – коэффициент корреляции между i-м и j-м признаками, где n – количество признаков, а D_i – дисперсия i-го признака.

На основе матрицы R строится граф (рис.1), вершинами которого являются первичные признаки, а ребру, соединяющему i-ю и j-ю вершины, ставится в соответствие модуль коэффициента корреляции.

Задавая произвольным образом или на основании предварительного изучения корреляционной матрицы некоторое пороговое значение r_o, из графа исключаются все ребра, которые соответствуют коэффициентам корреляции по модулю меньшим r_o. В результате граф распадается на несколько групп, связи между которыми отсутствуют (рис.2). Очевидно, что для полученных таким образом плеяд внутриплеядные коэффициенты корреляции будут больше r_o, а межплеядные – меньше r_o.

Среди признаков, входящих в плеяду, выбирается эталонный признак, поведение которого наиболее точно отражает поведение всех признаков плеяды (в случае высокой внутриплеядной связи эталонным можно выбрать любой из признаков плеяды). Эталонный признак становится тем новым фактором, который будет «представлять» плеяду в новом словаре. Таким образом, получаются новые непосредственно измеряемые факторы, количество которых равно количеству корреляционных плеяд, и меньше количества первичных признаков. В случае сильной внутриплеядной связи поведение фактора достаточно точно характеризует поведение всех признаков плеяды.

Однозначно определить границу «сильной связи» трудно. Рекомендуемый литературой [1] для задач распознавания образов пороговый уровень корреляции r_o должен быть не ниже 0,85 – 0,9. Использование данных параметров границы при построении системы обнаружения вторжений в КС дало возможность снизить размерность признакового пространства в два раза.

[1] Рамеев О.А, Коваленко А.П. //Методы анализа многомерных данных /Ред. Толстов В.Г., Иванов Б.И. – Москва, 1988. 621с.

ВОЗМОЖНОСТИ ЧИСЛОВОГО КОДИРОВАНИЯ В РАДИОТЕЛЕМЕТРИИ

О.В.Пустовалов, А.В.Силин

Нижегородский госуниверситет

При внедрении цифровых способов передачи информации в радиотелеметрию следует обратить внимание на принципиальную особенность телеметрической информации: она является результатом измерений и представляет собой последовательность чисел. С учетом этого обстоятельства в докладе предлагается специальный вид кодирования – числовое кодирование и обсуждаются возможности его использования в радиотелеметрических каналах.

При традиционном блочном кодировании с использованием корректирующих кодов (n, k), где k – число информационных символов, а n-k – число проверочных, возникающие из-за действия помех ошибки, проявляются при приеме в том, что вместо переданного сообщения a регистрируется b, c или d. При этом вопрос о том, что больше a-b, или a-d, лишен смысла. Однако, если a,b, c … d – числа, то поставленный вопрос имеет принципиальное значение. Числовое кодирование нацелено, прежде всего, на снижение величины ошибок, особенно больших.

Пусть передаче подлежит функция $X(t)$, описывающая изменение во времени некоторого технологического параметра. Будем полагать, что $X(t)$ – случайная функция с нормальным распределением мгновенных значений в диапазоне $D=x_{max}-x_{min}$, со средним значением $\bar{x} = D/2$. При заданной погрешности измерения $|\Delta x|$ находим шаг квантования $h=2|\Delta x|$, число уровней квантования M и необходимое число разрядов k при двоичной записи квантованных значений X_m (m=1,….M):

$$M = D / h,\ k = \log_2 M.$$

Величины X_m составляют статистический ряд [1]. Каждая составляющая этого ряда X_m появляется с вероятностью P_m, при этом очевидно:

$$\sum_{m=1}^{M} P_m = 1 .$$

Гистограмма распределения случайных X_m (рис. 1) вписывается в кривую распределения плотности вероятности X.

Каждое двоичное число можно рассматривать как кодовую комбинацию, а совокупность всех M комбинаций – как исходный код без избыточности. При этом в каждой комбинации сохраняется иерархия разрядов, присущая числам.

Ошибки, возникающие при приеме, проявляются в инверсии $1\underset{\leftarrow}{\rightarrow}0$ в одном или нескольких разрядах. Пусть ошибка произошла в старшем разряде. При этом, если $m \le M/2$, то ошибочное значение будет равным $m+\Delta_k$; если $m>M/2$, то ошибочное значение $\Delta_k - m$. Очевидно, что среднее значение ошибки равно нулю, а ее абсолютная величина $\Delta_k=M/2$. Поскольку наиболее вероятным значениям $m \le M/2$ будут соответствовать ошибочные значения $m+\Delta_k \approx M$, то именно они будут наиболее

вероятными. Аналогично, наибольшие вероятности будут также иметь ошибочные значения Δ_k- m при $m \to 1$. В соответствии с этим распределение ошибочных значений принимает вид рис. 2 (кривая s=k).

Анализируя одиночные ошибки в других разрядах, получим:

$$\Delta_s = M \cdot 2^{-k+s} = 2^{s-1}, \quad s = \overline{1,k}.$$

При одиночных ошибках в s – разряде максимумы функций распределения ошибочных значений будут симметрично относительно $M/2$ смещены в окрестности значений m_s' и m_s'' (см. рис. 2).

$$m_s' = \frac{M}{2} + 1 - \Delta_s = 2^{k-1} - 2^{s-1} + 1; \qquad m_s'' = \frac{M}{2} + \Delta_s = 2^{k-1} + 2^{s-1}.$$

Очевидно, что ошибка Δ_s, допущенная при приеме сигнала, равносильна ошибке измерения с погрешностью равной

$$\Delta x_s = \pm \Delta_s h \pm 0{,}5h = |\Delta \cdot 2^{s-k-1} \pm \Delta x|.$$

Продолжив анализ на случай кратных ошибок при приеме, приходим к выводу о необходимости при цифровой передаче числовой информации максимальным образом защищать от ошибок старшие разряды кодовых комбинаций. С этой целью, в частности, предлагается ресурс корректирующего кода (число разрядов n) распределять по разрядам двоичных чисел:

$$n = \sum_{s=1}^{k} n_s, \qquad n_k > n_{k-1} n_{k-2} \cdots > n_1,$$

создавая таким образом в каждом разряде свою информационную избыточность для передачи двух «микрособщений» 0 и 1. На базе n_s для каждого разряда выбирается по два варианта последовательного составного сигнала [2]. Суммарная длительность сигнала для передачи любого числа из M составит n символов. В приемнике при известных структурах сигналов используется взаимнокорреляционный метод приема с когерентным накоплением. Это обеспечит приоритетное снижение вероятности ошибок в старших разрядах принимаемых двоичных чисел.

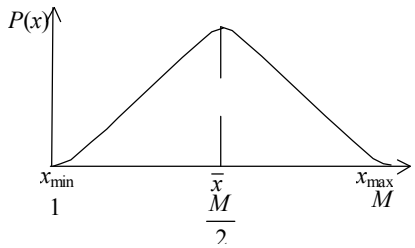


Рис. 1

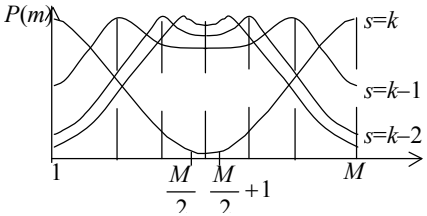


Рис. 2

[1] Вентцель Е.С. Теория вероятности. –М.: Наука, 1964.

[2] Варакин Л.Е. Системы связи с шумоподобными сигналами. –М.: Радио и связь, 1985.

РЕАЛИЗАЦИЯ АППАРАТНОГО CIL ПРОЦЕССОРА С НИЗКИМ ЭНЕРГОПОТРЕБЛЕНИЕМ

Д.К.Мордвинов, Д.В.Рагозин, М.А.Соколов, М.О.Шуралёв

Нижегородский госуниверситет

Парадигма .NET, разработанная фирмой Microsoft, представляет собой попытку создания универсальной интеграционной платформы, пригодной для широкого круга вычислительных устройств и бизнес-приложений, ориентированных на работу в Интернет. В отличие от платформы Java, используемое в .NET промежуточное представление программы в коде CIL утяжелено проверкой безопасности выполнения программы. Представление CIL содержит информацию об объектной модели программы в виде таблиц метаинформации, описывающих объявленные типы данных (классы), их иерархию, интерфейсы, и прочую информацию о программе. Динамическая память управляется с помощью сборщика мусора. Базовой для системы команд CIL является абстрактная стековая машина, что позволяет достаточно просто реализовать кроссплатформенность виртуальной машины.

Удобства модели CIL вызывают значительное уменьшение скорости исполнения программы. На ПЭВМ этот эффект компенсируется трансляцией CIL в коды процессора ПЭВМ, но такой подход малоприменим в мобильных устройствах. Большинство алгоритмов медиа-обработки и телекоммуникаций неэффективно выражаются на языке CIL и неэффективно транслируются в коды целевого процессора. Миграцию платформы .NET на мобильные устройства сдерживают объективные факторы низкой эффективности ПО (как по производительности, так и по энергопотреблению) в коде CIL. Одним из приемлемых решений этой проблемы является использование процессора, умеющего прямо исполнять код CIL и использовать метаинформацию «на лету». Низкопотребляющий CIL процессор может быть интегрирован в мобильные устройства, что позволит использовать маломощные вычислительные устройства для решения типичных клиент-серверных задач.

Архитектура процессора является определяющей для таких характеристик, как энергопотребление и скорость исполнения операций. Ограничения по энергопотреблению сужают выбор архитектуры до встраиваемых контроллеров и процессоров цифровой обработки сигналов (ПЦОС), из них фактически показывают высокую производительность в медиа-задачах лишь ПЦОС, часто используемые в мобильных устройствах.

Разработанные нами решения [1], [2] позволяют эффективно отобразить стек CIL-машины на регистровый фал ПЦОС. Ядро CIL процессора разрабатывается на базе ядра ПЦОС с встроенным дополнительным декодером CIL команд. Ядро ПЦОС расширяется для поддержки характерных операций объектной модели: доступа к полям и методам класса, проверки типов во время исполнения, поли-

морфных операций. Структура программной системы на базе CIL процессора показана на рис. 1, а структурная схема конвейера CIL процессора показана на рис. 2. Процессор состоит из исполнительного узла, декодера команд ПЦОС, конвейера CIL инструкций, декодера CIL инструкций и кеш-памяти метаданных. Процессор поддерживает одновременно два набора инструкций: ПЦОС и CIL. Декодер инструкций ПЦОС построен по классической 3-х ступенчатой схеме: «выборка – декодирование – исполнение». Для декодирования CIL инструкции вводится виртуальный указатель вершины стека *TOS*, указывающий, какой из регистров является его вершиной. Каждому физическому регистру сопоставляется логический номер элемента стека, регистровый файл параллельно с выполнением команд синхронизируется с стеком, находящимся в памяти.

Так как накладные расходы на обработку таблиц метаинформации во время исполнения могут оказаться слишком большими, решено преобразовывать наиболее важную метаинформацию в удобный для использования во время исполнения вид. Наиболее часто используемые её части хранятся в кеш-памяти метаданных. При минимальной реализации оптимизируются наиболее часто используемые инструкции CIL.

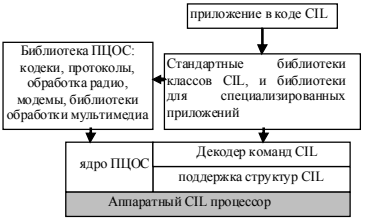


Рис. 1

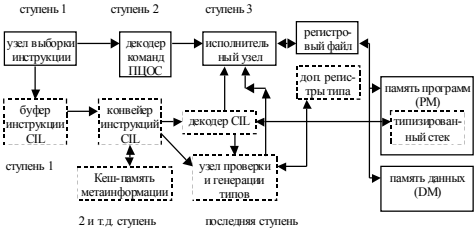


Рис. 2

Достаточно большая часть поддержки исполнения CIL кода выполняется с помощью программного обеспечения. Можно выделить несколько его основных составляющих: 1) *микрокод обработки исключений* – код ПЦОС, исполняющий CIL команды, аппаратная реализация которых затруднительна; 2) *библиотека классов* для обеспечения базовой функциональности; 3) *библиотеки поддержки платформы*; 4) *библиотеки поддержки обработки медиа-данных*; 5) *пользовательские приложения*.

Предлагаемая реализация CIL процессора удачно сочетает в себе процессор цифровой обработки сигналов и аппаратную эмуляцию стековой машины. Аппаратная реализация ПЦОС спроектирована с целью максимального уменьшения энергопотребления процессора. Реализация CIL производится на базе макетной платы ML-401 с чипом Virtex-4 LX-25 фирмы Xilinx, имеющим более 25000 логических вентилей.

[1] A. Chapyzhenka, S. Cherhyshow, D. Ragozin, A. Umnov. Low-power architecture for CIL-code hardware processor. //Technical report #1 on RFP2 project “Hardware CIL processor”. NNSU, September, 2004, 14 p.
[2] D. Ragozin, A. Umnov, A. Eltsov. Implementation of complex CIL instructions in the CIL hardware processor //Technical report #2 on RFP2 project “Hardware CIL processor”. NNSU, December, 2004, 8 p.

ОПТИМИЗАЦИЯ РЕШЕНИЯ ЗАДАЧИ ОПРЕДЕЛЕНИЯ ЭФФЕКТИВНОСТИ СИСТЕМ ПАРОЛЬНОЙ ЗАЩИТЫ НА ОСНОВЕ ГЕНЕТИЧЕСКИХ АЛГОРИТМОВ

А.Ю.Горбунов

Нижегородский государственный университет им. Н.И. Лобачевского

Актуальность задачи определения эффективности парольной защиты (ПЗ) обусловлена широким применением механизма ПЗ в современных операционных системах. Целью определения эффективности ПЗ является определение времени, необходимого на взлом ПЗ. Поскольку наиболее часто механизм ПЗ реализуется на основе криптографических алгоритмов хэширования, то задача определения эффективности ПЗ сводится к задаче определения эффективности (криптостойкости) алгоритмов хэширования.

Как известно, алгоритмы хэширования обладают двумя свойствами – ресурсоемкостью задачи подбора по заданному значению хэш-функции (свертки) исходного сообщения (необратимость) и ресурсоемкостью задачи поиска двух сообщений, значения сверток которых совпадают (стойкость к коллизиям). Из теории вероятности известно, что задача поиска коллизий является менее ресурсоемкой (парадокс дней рождения).

Для решения поставленной задачи предлагается использовать метод адаптивного поиска на основе генетических алгоритмов. Генетические алгоритмы широко описаны в литературе [1, 2] и доказана целесообразность их применения для решения задачи определения эффективности ПЗ [3].

Поскольку генетические алгоритмы предназначены для поиска оптимального решения (фенотипа) на заданном дискретном множестве (области поиска), представляемом в виде множества бинарных строк фиксированной длины (прообраз, называемый генотипом). Оптимальность определяется по степени приспособленности – значению целевой функции, заданной в области поиска и определяемой поставленной задачей.

Поскольку в механизмах ПЗ используются алгоритмы хэширования на основе одношаговых сжимающих функций, то в качестве прообраза целесообразно взять бинарные строки размером, равным удвоенной длине сообщения, принимаемого на вход сжимающей функцией (фактически прообраз представляет собой пару исходных сообщений). Тогда значение приспособленности (целевая функция) пропорционально количеству несовпадающих бит в свертках двух сообщений из прообраза.

Рассмотрим два произвольным образом выбранных сообщения M_i и M_j. Им соответствуют свертки H_i и H_j. Обозначим количество несовпадающих бит в H_i и H_j как r_{ij}. Очевидно, $r_{ij} \subseteq [0, n]$, где n – длина свертки (количество бит). Тогда вероятность события p_{ij}^r, состоящего в том, что для пары M_i и M_j количество несовпадающих бит в свертках H_i и H_j равно r определяется следующим образом:

$$p_{ij}^r = \frac{C_n^r}{2^n} \qquad (1)$$

Знание характера распределения (1) p_{ij}^r для конкретного алгоритма хэширования, можно определить минимальный размер популяции, для которого могут быть найдены коллизии. Например, для n = 128 (MD5) минимальный размер популяции составляет 132 особи.

После того как задача поиска коллизий сформулирована, возникает вопрос оптимизации решения задачи, то есть снижения ее ресурсоемкости – количества времени поиска коллизий и снижения требования к машинному ресурсу (оперативной памяти).

В качестве параметров оптимизации поставленной задачи могут выступать реализация генетического алгоритма (распараллеливание процессов естественного отбора, кроссовера и мутации), выбор алгоритма естественного отбора (рулеточный, турнирный или другой), выбор алгоритмов мутации и кроссовера (одно- или многоточечные алгоритмы) а также численность популяции.

Методы распараллеливания генетических алгоритмов на настоящий момент достаточно широко изучаются и также исследуется влияние распараллеливания на скорость работы алгоритма [4]. На основе экспериментальных данных для различных типов алгоритмов хэширования можно сделать вывод, что для поиска коллизий наибольшей эффективностью отличается турнирный метод естественного отбора. Применение различных видов кроссовера и мутации также широко исследовано [5] и применительно к поставленной задаче можно использовать различные виды многоточечного кроссовера для управления сходимостью генетического алгоритма. Численность популяции определяется исследуемым алгоритмом хэширования (длиной свертки n) с учетом распределения (1).

[1] Goldberg D.E. Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley, Reading, MA, 1989.
[2] Holland J.H. Adaptation in Natural and Artificial Systems. MIT Press, Cambridge, MA, 2nd edition, 1992.
[3] Горбунов А.Ю. //В кн.: Тр. (седьмой) научной конференции по радиофизике, посвященной 90-летию со дня рождения В.С. Троицкого. 7 мая 2003 г. /Ред. А.В.Якимов. –Нижний Новгород: ТАЛАМ, 2003. с.277
[4] Родзин С.И. // Перспективные информационные технологии и интеллектуальные системы. 2002. № 1. с.36.

[5] Spears, W., K. De Jong, T. Back, D. Fogel, and H. de Garis (1993). An overview of evolutionary computation. In European Conference on Machine Learning Volume 667, pp. 442-459. Springer Verlag.

СКРЫТОЕ МУЛЬТИПЛЕКСИРОВАНИЕ ПАРАЛЛЕЛЬНОЙ ШИНЫ.

А.В.Горюнов

Институт Физики Микроструктур РАН

На распространённых параллельных шинах объединяющих цифровые системы (общая шина – рис.1) есть состояние, когда все устройства шины отключены от линий адреса и данных [1]. В это время данные линии шины можно использовать для передачи сигналов, не вмешиваясь в стандартный протокол работы шины, т.е. сигналом мультиплексирования являются стандартные сигналы шины Управления. Это позволяет, используя только существующие линии сигналов общей шины, передавать дополнительные сигналы (ДС), например, прерывания.

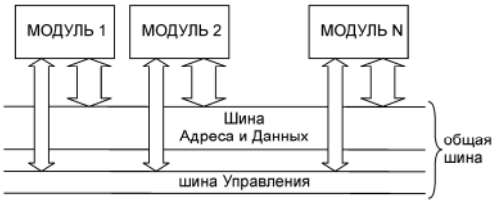


Рис. 1

При модификации уже существующих цифровых систем, использующих общую шину, можно изменить только отдельные, подключённые к общей шине, модули, не затрагивая остальные. При проектировании новой цифровой системы с использованием скрытого мультиплексирования параллельной шины сокращается энергопотребление и габариты и повышается надёжность счёт сокращения количества протяжённых линий и контактных групп разъёмов.

Недостатком является усложнение коммутации сигналов и появление задержек при передаче ДС (и только ДС). Возможно два основных способа подключения: непосредственно к общей шине, аналогично стандартному модулю и через мультиплексор (Рис. 2). Последний подход предпочтительнее, т.к. исключает дополнительный драйвер шины.

Схема «разрешения ДС» формирует сигнал *E* «разрешения передачи ДС» на шину и приёма с шины, когда по сигналам управления передающие драйверы остальных устройств отключены.

Схема «демультиплексирования ДС» восстанавливает ДС на приёмном конце. При этом необходимо предусмотреть защитные интервалы как после начала приёма (установления сигнала *E*), так и перед окончанием (снятием сигнала *E*) на время переходных процессов на шине и фиксацию на время запрета прохождения ДС.

Если передаваемые данные используются как сигнал прерывания по фронту [2], то при демультиплексировании нет необходимости дополнительно фиксировать сигнал, а достаточно запрещать активный уровень ДС на время запрета прохождения, что позволяет обойтись на каждый канал ДС одним тактируемым сдвиговым регистром с асинхронным сбросом [3].

Рис. 2

Данное условие выполняется для широкого спектра процессоров [1], в частности, для DSP процессора TMS320VC54xx [4], а для некоторых микроконтроллеров, например серии AVR фирмы Atmel требует специальной инициализации регистров управления прерываниями [5]. Поскольку данные микроконтроллеры при выполнении программы могут длительное время не обращаться к общей шине, а в фазе обращения к ней всё равно не могут приступить к обработке прерывания [4,5], то в системе с одним ведущим процессором задержка составляет только время переходных процессов на шине. Однако данная задержка происходит и в системе без мультиплексирования.

Таким образом, применение скрытого мультиплексирования параллельной шины для передачи сигналов прерывания по фронту не приводит к потере производительности цифровой системы.

Технология успешно применена при разработке 10–канального контроллера измерительной системы промышленного применения.

[1] Хвощ С.Т., Варлинский Н.Н., Попов Е.А. Микропроцессоры и микроэвм в системах автоматического управления.– Ленинрад: “Машиностроение”, 1987, 640с.
[2] Солонина А., Улахович Д., Яковлев Л. Алгоритмы и процессоры цифровой обработки сигналов. Санкт-Петербург: “БХВ-Петербург”, 2002, 464с.
[3] Шило В.Л. Популярные цифровые микросхемы. Челябинск: “Металлургия”, 1989, 352с.
[4] TMS320C54xx DSP Reference Set. Volume 1: CPU and Perepherals. Datasheet. USA,Texas Instruments, 1999г.

[5] 8-bit Microcontroller with 128K Bytes In-System Programmable Flash. Datasheet. USA, Atmel, 2002, 360c.

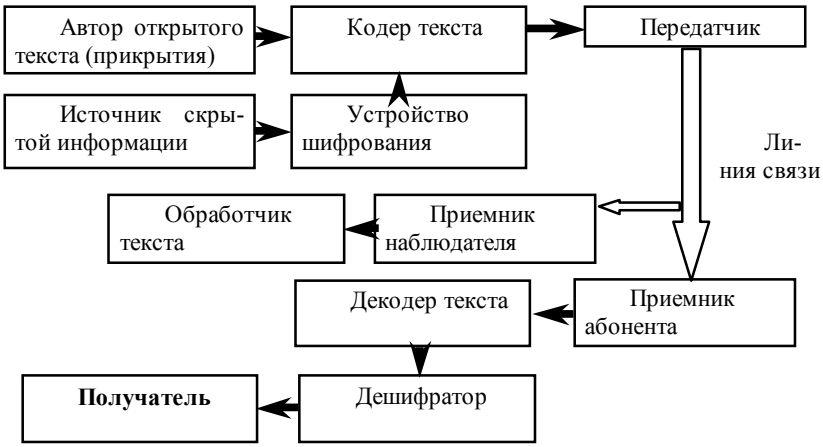
СКРЫТНАЯ ПЕРЕДАЧА ДАННЫХ В ТЕКСТОВЫХ СООБЩЕНИЯХ

С.Л.Моругин

Нижегородский государственный технический университет

Текстовые сообщения – один из наиболее доступных способов передачи информации (электронная почта, SMS-сообщения, письменный текст в составе вложений, письма на бумаге и др.).

Цель – скрытно передать зашифрованную информацию в составе открытого текстового сообщения, которое может быть перехвачено наблюдателем. Наблюдатель не должен сделать обоснованный вывод о наличии в тексте скрытой информации. Предполагаем, что дешифровать перехваченную информацию невозможно. Система передачи скрытой информации показана на рисунке



Предположения наблюдателя при анализе перехваченных сообщений:
- возможность наличия скрытой информации в тексте;
- методы и алгоритмы внесения в текст скрытой информации известны;
- стиль автора и контекст передаваемой информации известен.

Возможные выводы, полученные при анализе перехваченного сообщения:
- текст, скорее всего, содержит скрытую информацию;
- наличие скрытой информации в тексте не заметно и не вытекает из его анализа;
- текст имеет искусственное происхождение.

Задачи формирования текста со скрытой информацией:
- получение текста с *естественным логическим содержанием.* Передаваемый текст получается на основе естественного текста. Сохранение смысла текста

достигается смысловой эквивалентностью преобразованного и исходного текста.

- получение текста *квазиестественного происхождения*. Уменьшение искусственности достигается сбалансированностью статистических характеристик полученного текста и естественных текстов.

Проблема исследования – оценка пределов вариабельности различных естественных текстов по показателям, существенным для методов кодирования.

Оценки информационных свойства текста:

- энтропия искусственного текста (как набора произвольных слов) – 18…20 бит на одну словоформу;
- энтропия естественного текста с большим словарным запасом (Imax) – около 11,5 бит на одно слово-концепт (в текстах с малым словарным запасом энтропия на одно слово-концепт меньше);
- энтропия реального текста, набранного на одном регистре, около 17,7 бит на одну словоформу (по архиватору).

Два текста назовем *грубо эквивалентными*, если они приводятся один к другому по правилам грубой эквивалентности текста. Логический смысл двух грубо эквивалентных текстов близок.

Некоторые правила получения грубо эквивалентных текстов:

- замена слов синонимами:
- замена подчиненных предложений на причастные обороты:
- замена знаков препинания на эквивалентные или отсутствующие знаки:
- замена чисел на грубо эквивалентные, не приводящие к искажению смысла.

Информационные характеристики текста, грубо эквивалентного естественному:

- открытая информация на одно слово-концепт в тексте со словарно-групповым запасом 8000 групп концептов – около 9 бит;
- скрытая информация на одно слово при словарно-групповом запасе 8000 групп – 2,7 бит…2,3 бит;
- общая информация – 11,7…11,3 бит: $I_{сумм} = I_{скр} + I_{откр}$

Коэффициент передачи скрытой информации: $КПСИ = I_{скр}/I_{max}$.

Число групп слов-синонимов при словаре в 64000 слов-концептов	Число слов в наибольшей группе	Число слов в наименьшей группе	Скрытая информация на одно слово, бит	КПСИ при равновероятном выборе синонимов	КПСИ при не равновероятном выборе синонимов
16000	7	2	1,9	17%	14%
8000	21	2	2,7	24%	20%
4000	54	2	3,1	30%	25%
2000	121	3	4,3	37%	31%
1000	260	5	5,2	45%	38%

Выводы. Чем строже стиль автора текста, тем меньше скрытой информации можно поместить в текст. Стиль с произвольными искажениями и сокращениями слов дополнительно дает 3-4 (и более) бита передаваемой информации на слово.

Передача 10-15% скрытой информации от объема открытой практически не накладывает ограничений на формирование текстов и трудно обнаруживается.

СИНТЕЗ И РАСПОЗНАВАНИЕ ТЕКСТОВЫХ СООБЩЕНИЙ

С.Л.Моругин, А.А.Штанюк

Нижегородский государственный технический университет

Исследования в области компьютерной лингвистики давно привлекают внимание специалистов. Компьютерный анализ и синтез текстов на естественном языке (ЕЯ) или на ограниченном естественном языке (ОЕЯ) вызывают интерес по следующим причинам:

1) В настоящее время накоплен огромный массив электронных текстов, содержащих информацию по всем предметным областям человеческой деятельности.
2) Интерфейс с информационными системами на ЕЯ более дружественен пользователю, чем командный, или даже графический.
3) С ЕЯ-интерфейсом связано решение множества прикладных задач, включая анализ информационных потоков, работа с СУБД, с поисковыми системами Интернет.

Несмотря на ряд достигнутых успехов за рубежом в этой области, проблема синтеза и анализа текста является во многом зависимой от особенностей национального языка, что приводит к трудности применения имеющихся зарубежных разработок. Русский язык, с этой точки зрения, представляет ряд трудностей, поскольку для него характерен более свободный порядок слов в предложении, многообразие грамматических форм и наличие большого числа исключений.

Одним из способов борьбы с этими трудностями, является использование ОЕЯ. В этом случае фиксируется порядок слов в предложении, сокращается словарная база, снижается количество синонимов и омонимов в тексте. Кроме того, упрощается и само предложение, запрещаются сложные формы и обороты.

Построим математическую модель текста на ЕЯ.

Зададим последовательность слов-концептов Π из словаря:

$$\Pi = \{x_1, x_2, \ldots, x_m\}, \text{ где } x_1 \in G_1, x_2 \in G_2, \ldots, x_m \in G_m,$$

Зададим сигнатуру текста S – последовательность правил (операций) P_i, применяемых к последовательности слов-концептов:

(номер правила 1, параметры правила 1),…,

(номер правила n, параметры правила n)

У каждой операции P_i из множества допустимых операций P могут быть заданы параметры a_i.

Сигнатуру текста обозначим:

$$S = \{P_1(a_1), \ldots, P_n(a_n)\} \ . \ P_i \in P.$$

Текстовое выражение V образовано последовательностью слов-концептов и сигнатурой текста

$$V = \{П, S\}.$$

Предложение письменного текста как набор словоформ и разделителей – результат преобразования текстового выражения

$$T = F(V),$$

где F – оператор развертки (преобразования) текстового выражения в текст.

Каждое слово-понятие c_p по способу образования словоформ и сочетанию слов в предложении можно отнести к той или иной синтаксической категории G. Каждой последовательности слов-концептов $П$ соответствует последовательность синтаксических категорий слов-концептов

$$П_G = \{G_1, G_2, \ldots, G_m\}.$$

Грамматическая форма $Г$ текстового выражения (или предложения письменного текста) – последовательность синтаксических категорий и сигнатура текста.

$$Г = \{П_G, S\}, Г \in Q.$$

Q – множество допустимых грамматических форм.

Грамматические формы текста $Г1$ и $Г2$ - эквивалентные грамматические формы, если они приводят, при подстановке вместо категорий G любого слова x соответствующей категории, к эквивалентным текстовым выражениям

$$t_1 = t_2, \text{ где } t_1 = F(\{П_1(x), S_1\}),\ t_2 = F(\{П_2(x), S_2\}),\ \forall\, x \in G$$

и, далее, к одинаковым текстам.

Последовательность анализа текста может быть представлена в виде последовательности следующих шагов:

1) Выделение концептов.
2) Построение сигнатуры.
3) Построение графа предложения.
4) Соотнесение с библиотекой шаблонов.
5) Семантическая интерпретация.

Последовательность синтеза текста может быть представлена следующим образом:

1) Построение базового сообщения, несущего информацию.
2) Расширение базового сообщения.
3) Согласование сообщений друг с другом (формирование связного текста).

Базовое сообщение формируется на основе шаблона, хранящегося в библиотеке шаблонов. Каждый шаблон задает логическую или сущностную связь между некоторыми объектами. В базовом предложении содержится описание некоторого факта окружающей действительности, при этом предложение построено по всем правилам русского языка. Далее, предложение может быть расширено введением дополнительных речевых оборотов или уточнений, ему может быть придана соответствующая литературная окраска. И, наконец, при наличии последовательности предложений, требуется согласование одного предложения с другим для придания

связности тексту. В частности, могут использоваться местоимения и сокращения вместо наименований объектов.

К ПОСТРОЕНИЮ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ РАСПОЗНАВАНИЯ АЛГОРИТМОВ ПРОГРАММ

Д.Л.Туренко

Нижегородский государственный университет им. Н.И. Лобачевского

Восстановление алгоритмов программ по их исполняемому коду (ИК) является важной и актуальной проблемой при исследовании безопасности программного обеспечения (ПО) ЭВМ. Разработка эффективных методов решения данной проблемы позволит проводить идентификацию вредоносных программ, выявление недокументированных функций, а также поиск уязвимостей в системном и прикладном ПО.

Современные интегрированные визуальные пакеты разработки ПО предоставляют программисту богатые возможности по автоматизации создания программ. В процессе разработки программ широко используются библиотеки функций и шаблонов. Кроме того, программисты используют фундаментальные алгоритмы, стандартные приемы программирования. Поэтому программы содержат большую долю стандартного ИК, соответствующего библиотечным функциям, процедурам инициализации и устойчивым последовательностям операторов языка программирования («клише»).

К примеру, ИК тривиальной программы на языке C «Hello, World!», сгенерированный компилятором фирмы Microsoft версии 7.10, содержит около 7300 инструкций, и лишь 5 из них составляют код, написанный программистом.

При восстановлении алгоритмов программ или их отдельных функций возникает проблема идентификации стандартных блоков ИК, которую целесообразно проводить в автоматизированном режиме. Для этого необходимо построение и анализ математических моделей (ММ) ИК.

В рамках проводимых исследований были рассмотрены следующие ММ: граф вызовов функций (call-граф) [1], генетические карты [2] и управляющий ориентированный граф (control flow graph) [3]. Проводилось определение инвариантных характеристик и параметров ММ, которые бы позволяли идентифицировать блоки ИК (а значит и реализованные в них алгоритмы) при использовании различных компиляторов и языков программирования.

Основные результаты получены для ММ на основе управляющего ориентированного графа. Разработанные программные средства позволяют строить графы программ и их отдельных функций и проводить идентификацию блоков ИК, соответствующих этим функциям. Для решения проблемы восстановления алгоритмов программ предлагается следующая процедура автоматизированного анализа ИК:

1. Формируется база данных эталонных представителей классов реализаций множества библиотечных функций, стандартных процедур инициализации и «кли-

ше». Эффективность системы автоматизированного распознавания алгоритмов программ будет определяться полнотой данной «базы знаний».

2. Строится ММ исследуемой программы и производится поиск блоков ИК, соответствующих алгоритмам из «базы знаний».

3. Производится декомпозиция ММ исследуемой программы на функциональные блоки, сведение к ММ в виде call-графа и локализация фрагментов ИК, для дальнейшего анализа программистом.

Таким образом, целью автоматизации процесса исследования программы является построение ММ в виде call-графа – наиболее удобной для восприятия человеком ММ ИК.

При реализации предложенной процедуры могут возникнуть принципиальные трудности при построении ММ программ, связанные, например, с наличием динамически изменяемых управляющих структур, защиты ИК от исследования и др. Многие из этих трудностей удастся обойти, если в процессе построения ММ ИК получать не статический дисассемблированный код, а эмулировать работу программ.

Кроме того, решение прикладной задачи разработки удобного графического представления и визуализации полученных результатов позволит существенно помочь программисту в понимании алгоритма и структуры программы в целом.

В итоге, в процессе исследований подходов к автоматизированному распознаванию алгоритмов программ установлено, что:

- использование ММ в виде управляющего ориентированного графа позволяет проводить идентификацию алгоритмов в определенном классе реализаций;
- процесс идентификации алгоритмов требует предварительного построения базы данных эталонных представителей классов реализаций;
- предложенная процедура автоматизированного анализа ИК позволяет эффективно проводить идентификацию стандартных блоков ИК.

[1] Туренко Д.Л., Калинин С.В. //В кн. Труды Пятой научной конференции по радиофизике, ННГУ, 2001 г., с.357

[2] Туренко Д.Л., Кирьянов К.Г. // Вестник ННГУ. Серия “Радиофизика”, ННГУ, 2003 г., с.37

[3] Туренко Д.Л., Кирьянов К.Г.// Труды Всероссийской научно-технической конференции “Информационные системы и технологии” (ИСТ-2005), НГТУ, 2005 г., с.117

ГИБРИДНАЯ ИНТЕЛЛЕКТУАЛЬНАЯ СИСТЕМА "ДИНАМИКА РЕГИОНА"

В.А.Савин[1)], А.Т.Надеев[2)], О.С.Данилова[2)]

[1)]Нижегородский госуниверситет, [2)]Волго-Вятская академия госслужбы

Обеспечение интеллектуальной поддержки принятия управленческих решений на всех уровнях жизни общества было и остается актуальной задачей. Особая роль

при этом отводится информационно-компьютерным технологиям, позволяющим адекватно описывать динамику социально-экономической ситуации в обществе.

Целью настоящей работы явилась разработка математической модели и реализующего ее программного комплекса, позволяющих описывать основные социальные, хозяйственные и финансовые процессы отдельного региона (федерального округа, субъекта федерации, муниципального образования). В основу математической модели положено представление о регионе, как о сложном социально-экономическом объекте, состояние которого может быть описано иерархической системой показателей. Эти показатели в свою очередь зависят от ряда переменных, таких как например: численность городского и сельского населения по различным возрастным группам, объемы основных производственных фондов по отраслям и секторам экономики с учетом их физического состояния (новые, старые, ветхие), объемы производства в сопоставимых ценах по отраслям и секторам экономики, доходы и расходы бюджетов органов власти и хозяйствующих субъектов.

Динамику изменения во времени основных переменных, определяющих социально-экономическое состояние региона, предложено описывать системой дифференциальных уравнений следующего вида:

$$\begin{cases} \dfrac{dY_1}{dt} = \left(\delta Y_0 + \alpha Y_2\right) - \left(\mu_1 + \dfrac{1}{\tau_1}\right) Y_1, \\ \dfrac{dY_2}{dt} = \dfrac{Y_1}{\tau_1} - \left(\mu_2 + \dfrac{1}{\tau_2}\right) Y_2, \\ \dfrac{dY_3}{dt} = \dfrac{Y_2}{\tau_2} - \left(\mu_3 + \dfrac{\delta}{\tau_3}\right) Y_3. \end{cases}$$

Здесь первые слагаемые правых частей дифференциальных уравнений описывают рост основных переменных (за счет инвестиций, рождаемости), в то время как вторые – естественную их убыль (старение, смертность).

Помимо приведенных уравнений, математическая модель включает в себя балансовые соотношения различных видов ресурсов и функциональные связи между переменными и параметрами модели региона. Это, например, балансы по доходам и расходам регионального бюджета и хозяйствующих субъектов, балансы распределения трудовых ресурсов по отраслям и секторам экономики региона, балансы затрат ресурсов и объемов выпуска продукции. Группы уравнений, описывающих функциональные связи, моделируют зависимости:

- степени износа основных производственных фондов от инвестиций;
- производительности труда от состояния производственных фондов;
- доходов трудящихся от производительности и объемов производства;
- темпов рождаемости и смертности от уровня доходов населения;
- уровня преступности от уровня занятости и среднедушевых доходов.

Рассмотренная модель реализована в виде программного комплекса "Динамика региона", представляющего собой систему из 5 основных модулей (рис.1).

Наличие модуля "Принятие решений" обеспечивает активное участие пользователей в работе комплекса, делает ее открытой, игровой, а весь программный комплекс превращает в гибридную систему. Модули комплекса программно реализованы в виде иерархической блочной структуры с разбиением по отраслям и секторам экономики и органам управления (власти). Общим управляющим модулем комплекса является блок "Администратор". Подобная организация позволяет осуществлять работу комплекса (включая сетевой вариант) в различных режимах: a) анализ ситуации; b) оценка и принятие решений; c) синтез решения; d) прогнозирование.

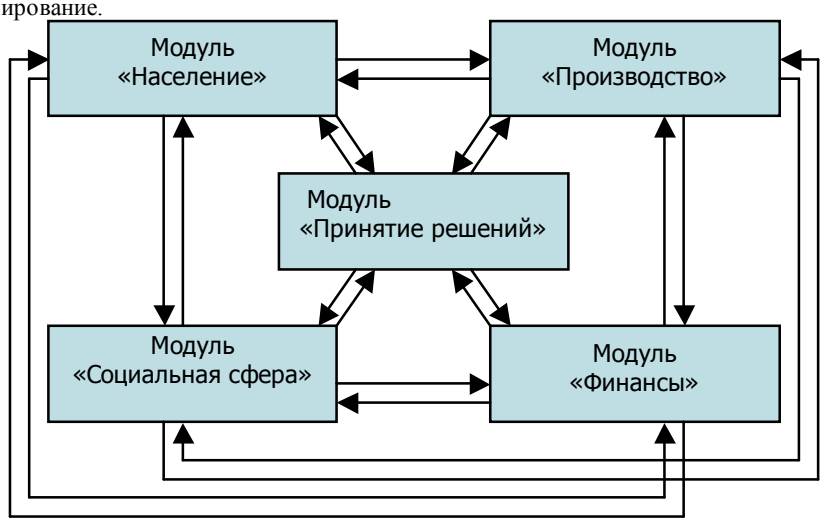


Рис. 1

В ходе тестирования разработанного программного комплекса на известных, но, к сожалению, не всегда достоверных данных статистики по динамике социально-экономической ситуации в Нижегородской области, ошибки результатов математического моделирования не превосходили 10%.

ОБ ОПРЕДЕЛЕНИИ ДОСТАТОЧНОГО ЧИСЛА ОТВЕДЕНИЙ С ИЗУЧАЕМОЙ ДИНАМИЧЕСКОЙ СИСТЕМЫ.

Кирьянов К.Г.[1)], Грунина Е.А.[2)]

[1)]Нижегородский госуниверситет, [2)]Нижегородская медицинская академия

Традиционные методы определения («оценки») достаточного числа отведений с изучаемого объекта имеет большую историю, и остаются, по сей день, весьма актуальными, так как разработанные методы (в физике, химии, биологии, медицине и т.д.) не одинаково эффективно применимы к различным объектам даже одной и той же природы (из-за многообразия исходных представлений о фактической «сложности» объекта, его «зашумлённости» и, как следствие, возможной неадекватности его математической модели /ММ/ по отношению к действительности). Задача определения достаточного числа отведений в ряде разделов науки и техники связана с определением числа и значений информативных параметров, контрольных точек, и т.д. и т.п.).

Для дальнейшего нам не важна полная информация о конкретном виде приводимых ниже уравнений (1) и (2) ММ изучаемого объекта (а, точнее, изучаемой подсистемы рис.1 более сложной системы) из теории дискретных динамических систем (ДДС), представимых в стандартной форме

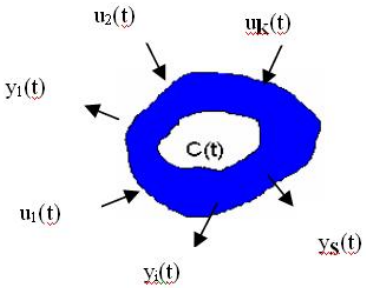
$$\mathbf{c}(t+\Delta t) = D(\mathbf{u}(t); P(\Delta t, q, n; \mathbf{p}))\mathbf{c}(t), \qquad \mathbf{c}(0) = \mathbf{c_0} \tag{1}$$

$$\mathbf{y}(t) = H(\mathbf{c}(t), P(\ldots)), \tag{2}$$

(где t – время, **u(t), c(t) и y(t),** D, H, P – соответственно, векторные «вход», «состояние», «выход», оператор динамики, функция наблюдения и параметр подсистемы), а важно лишь предположение о том, что эти уравнения существуют и адекватно описывают поведение изучаемого объекта. Наличие информации об объекте технической, медицинской и др. природы всегда приводит к уравнениям в такой форме.

Нам для дальнейшего важно, чтобы подсистема рис.1 как часть некоторой «большой» системы (объекта) была:

- либо изначально автономна (стационарна)**,** т.е. вектор **u(t)** «входа» имеет компоненты $u_j=0$, j=1,2,…,k**,**
- либо её ММ могла быть приведена к автономной за счет расширения границ подсистемы, т.е. увеличения числа n компонент вектора внутреннего состояния **c(t)** за счет присоединения компонент уравнений динамики для **u(t).**



Автономная или приведенная к автономной подсистема рис.1 позволяет:

- наблюдается с помощью «выходных» непрерывных или квантованных по времени векторного процесса $\mathbf{y}(t)\equiv\mathbf{y}(m\cdot\Delta t)$, $i=1,2,\ldots,\mathbf{s}$, Δt-шаг квантования по времени, на «представительной» длине $m=0,1,2,\ldots,\mathbf{M}$ = целая часть$\{T/\Delta t\}$**;**
- оценивать наборы оптимальных базовых параметров $(\mathbf{q}_i, \mathbf{n}_i)$ $i=1,2,\ldots,n$ с каждой из *скалярных* компонент $y_{i,m}$ «выходных» *векторного* процесса $\mathbf{y}(t)\equiv\mathbf{y}(m\cdot\Delta t)$ [1,2]**;**
- выбирать максимальный базовый параметр $(n_i)_{max}=\mathbf{n}_{max}$ из полученного набора n_i. Он будет характеризовать «сложность» или число компонент n внутреннего состояния $\mathbf{c}(t)$ с точностью («грубостью») порядка $1/\mathbf{q}_{min}$[2]**;**
- предположить в силу свойств функции наблюдения H(.) (2), что число выходов y_i , $i=1,2,\ldots,s$ с точностью («грубостью») порядка $const\cdot(1/\mathbf{q}_{min})$ равно $\mathbf{n}_{max}$

$$s=\mathbf{n}_{max}\ ; \tag{3}$$

- вычислить «интегральные» наборы $\mathbf{I}$ оптимальных базовых параметров $(\mathbf{q}_I, \mathbf{n}_I)$ *векторных* процессов с произвольным набором из *скалярных* компонент $y_{i,m}$ "выходных" *векторных* процессов y_i , $i=1,2,\ldots,s$**;**
- перебрать варианты наборов из, самое большее, $\mathbf{n}_{max}$ различных *скалярных* компонент $y_{i,m}$, выбрав из них набор $\mathbf{I}=(i_1,i_2,i_3,\ldots,i_f)$ с минимальными $\mathbf{n}_I=(\mathbf{n}_I)_{min}$ **и** $(1/\mathbf{q}_I)=(1/\mathbf{q}_I)_{min}$.
- установить, что если

$$(n_I)_{min}=1, \tag{4}$$

то набор $\mathbf{I}$ позволяет выбрать не только достаточное *число* $\mathbf{f}$ отведений (контрольных точек, информативных отводов и т.д.) подсистемы, но и указать конкретные искомые отведения $\mathbf{y}_i$, $i=i_1, i_2,\ldots,i_f$ (контрольные выходы)**.** Если же

$$\mathbf{n}_{max}\geq(n_I)_{min}>1, \tag{5}$$

то однозначный диагноз поведения по любому из наборов по $(\mathbf{n}_I)_{min}$ отведений установить нельзя. Можно, однако, пытаться повторить процедуру с отведениями взятыми и с других точек объекта, и фактически связанных с той же подсистемой.

Предложенный метод успешно опробован на ряде ММ дискретных технических систем и непрерывных ММ природных и медицинских объектов.

[1] Kiryanov K.G. To a choice of the basic parameters of mathematical model of experimental data. Proceedings 5-th International Specialist Workshop in area Nonlinear Dynamics Of Electronic Sistems. Moscow, Russia, 26-27 June 1997, pp. 400-403.

[2] К.Г. Кирьянов. Выбор оптимальных базовых параметров источников экспериментальных данных при их идентификации. Труды III Международ. конф. «Идентификация систем и задачи управления» SICPRO'04. М.: ИПУ РАН. 2004. С.187-208.

ПРЕДПОСЫЛКИ ДЛЯ СОЗДАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ОБРАБОТКИ ДВУХМЕРНЫХ ИЗОБРАЖЕНИЙ В РЕВМАТОЛОГИИ

Е.А.Грунина [1], К.Г.Кирьянов [2]

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

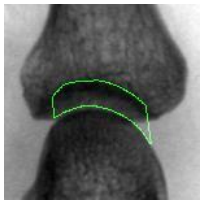
Ревматоидный артрит (РА) – это воспалительное ревматическое заболевание неизвестной этиологии, характеризующееся симметричным хроническим эрозивным артритом периферических суставов и системным воспалительным поражением внутренних органов [1]. РА является самым частым аутоиммунным заболеванием человека и характеризуется воспалением и прогрессирующей деструкцией суставов со значительным нарушением их функции. Он поражает людей любого возраста, в том числе наиболее трудоспособного, имеет тенденцию к неуклонному прогрессированию и очень часто приводит к инвалидизации. Показатели инвалидности и смертности у больных РА сопоставимы с таковыми при сахарном диабете ишемической болезни сердца с выраженным атеросклерозом коронарных сосудов.

Доменами ревматоидного артрита являются: активность воспаления, повреждение суставов, функция суставов, прямые и непрямые затраты, качество жизни. Ревматоидный артрит 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 актуальным стала 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 Ван дер Хайде [2].

До сих пор оценка ренгенограмм не автоматизирована, ее проводит врач вручную. Австрийскими авторами [3] сделана попытка автоматизировать ввод результатов оценки в специальные электронные формы, что ускоряет процесс обработки данных на 25%, но при этом сама обработка данных не автоматизирована.

В настоящее время проблемы автоматизации рентгенологическая оценка суставной деструкции связаны со сложностями на ряде этапов:

1) Автоматическое выделение набора суставов для оценки.
2) Оценка ширины и площади суставной щели.
3) Обнаружение эрозий (краевых дефектов) кости.
4) Оценка количества и площади эрозий.



Промежуточным решением первой проблемы будет определение суставов врачом на экране монитора компьютера.

Оценка ширины и площади суставной щели включает:

- Моделирование 3D изображения
- Обводка «переднего» края кости
- Определение «боковых краев» суставной щели
- Измерение ширины и площади щели
- Сравнение с нормальными показателями

Пример решения этой задачи показан на рисунке.

Обнаружение эрозий может проводиться автоматизировано. 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 проведены магистрантом НГТУ под руководством профессора Кирьянова К.Г. 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 делает возможным после набора статистики полуавтоматического анализа состояния сустава. Полуавтоматического, 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.

В ходе работы над программой выделены дополнительные признаки для автоматизации: оценка пространственного распределения эрозий, остеопения – разрежение кости в области пораженного сустава, кисты – округлые дефекты кости, не выходящие на край, при отсутствии суставной щели – диагностика анкилоза (сращения костей), диагностика подвывихов. При решении этого ряда задач работа автоматизированной системы выйдет за рамки оценки костно-суставной деструкции и станет возможной дифференциальная диагностика ревматоидного артрита и ряда других суставных заболеваний.

[1] Рациональная фармакотерапия ревматических заболеваний: Рук. Для практикующих врачей / В.А.Насонова, Е.Л.Насонов, Р.Т.Алекперов и др.; под общ. ред. В.А.Насоновой, Е.Л.Насонова. – М.: Литтерра, 2003. – с.87.

[2] Interpreting radiographic data in rheumatoid arthritis. P.A.Ory //Ann Rheum Dis 2003; 62: 597-604.

[3] Ph. Peloschek, F. Kainberger The RheumaCoach – a new approach to score rheumatoid arthritis http://www.univie.ac.at/radio/radio.htm Viewed 28/04/2004.

ВИРТУАЛЬНЫЙ АНАЛИЗАТОР СВЧ ЦЕПЕЙ

А.В.Беднов, С.М.Никулин, А.М.Кудрявцев

Нижегородский государственный технический университет

Компьютеры в наше время становятся не только вычислительными средствами, они превращаются в универсальные виртуальные измерительные приборы. Устройства на основе персонального компьютера (ПК) – заменят стандартные измерительные приборы: вольтметры, осциллографы, магнитографы, анализаторы спектра и другие, на систему виртуальных приборов [1]. Компьютер (обычно IBM-совместимый, настольный или портативный) как центральный орган любой виртуальной измерительной системы выполняет, прежде всего, функции интерфейса «человек-объект измерения». Кроме того, любой ПК обладает большой вычислительной мощностью, которую можно использовать для обработки результатов измерений. По-существу, виртуальные приборы стали стандартом в измерительной технологии, особенно при измерениях на высоких и сверхвысоких частотах.

Современный анализатор СВЧ цепей состоит из двух частей:

a) платы сбора данных (DAQ-board)
b) специализированной измерительной интегрированной программной оболочки для хранения, обработки и визуального представления измерительной информации, например, LabVIEW.

Использование такой двухуровневой архитектуры позволяет наиболее полно использовать алгоритмы цифровой и математической обработки данных без потери функциональной гибкости и наглядности представления результатов измерений, характерной для традиционных анализаторов цепей.

Между тем, возможности цифровой обработки данных могут быть использованы не только при работе с существующими физически анализаторами цепей, но и в процессе моделирования устройств, блоков и схем. Фактически, для конечного пользователя виртуального анализатора стирается жесткая грань между измерениями и моделированием. Одни и те же средства измерения человек может использовать как для традиционной обработки данных, полученных через DAQ-board, так и виртуальных, полученных из программы, моделирующей работу разрабатываемого прибора. Неоценимый вклад в развитие программных комплексов такого вида вносит технология интеграции программного обеспечения посредством COM, DCOM, COM+, .NET и т.д. При проектировании структуры интегрирующего программного обеспечения необходимо минимизировать зависимость разрабатываемой программы от конкретных реализаций измерительных приборов как реальных, так и виртуальных (рис.1). Только в этом

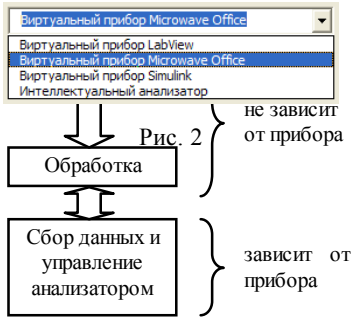


Рис. 1

случае реализация взаимодействия программного обеспечения анализатора с любой из моделирующих программ будет соответствовать общему подходу, характерному для использования интегрирующего виртуального анализа.

Рассмотрим интеграцию анализатора цепей с многоканальными рефлектометрами и системы математического моделирования AWR Design Environment (Microwave Office) компании Applied Wave Research, Inc.

Рефлектометры извлекают информацию о волновых параметрах объектов в широком динамическом диапазоне при различных режимах детектирования, которые задаются только формой зондирующих сигналов [2]. Microwave Office позволяет работать как с линейными, так и с нелинейными моделями рефлектометров.

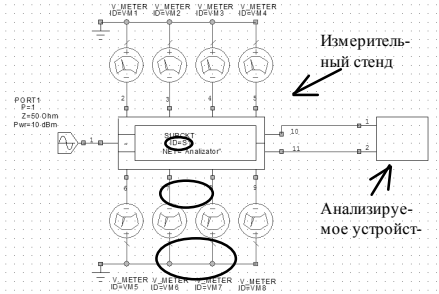


Рис. 3

Общий принцип измерений с помощью анализатора предполагает:

1) моделирование разрабатываемого устройства в программе microwave office;
2) запуск программного обеспечения виртуального анализатора и выбор интересующей модели как показано на рисунке 2 (при этом в проекте Microwave office автоматически создается виртуальный измерительный стенд, показанный на рисунке 3);
3) подключение виртуального устройства к измерительному стенду и запуск процесса измерения.

[1] Гёлль П. Как превратить персональный компьютер в измерительный комплекс: Пер. с франц. - 2-е изд., испр. - М.: ДМК, 1999. - 144 с.
[2] Налькин М.Е., Никулин С.М., Пугин М.В., Хилов В.П. Анализатор СВЧ цепей с амплитудным и гомодинным детектированием сигналов. Датчики и системы, 2003, № 7(50), с.13-16.

ИЗМЕРЕНИЕ И ИДЕНТИФИКАЦИЯ ПАРАМЕТРОВ НЕЛИНЕЙНЫХ СВЧ-ТРАНЗИСТОРОВ И ДИОДОВ

А.М.Кудрявцев[1)], Ю.В.Кузьмина[2)], И.Н.Малышев[2)], С.М.Никулин[2)]

[1)] ФГУП ННИПИ «Кварц»

[2)] Нижегородский государственный технический университет

Проблема корректного восстановления S-параметров СВЧ-транзисторов и диодов состоит в том, что, при заданной амплитуде $|a_1| = const$ и известных импедансах внешних цепей, экспериментально можно определить лишь две величины. Это коэффициент усиления K или преобразования $K_{пр}$ и входной коэффициент отражения $\Gamma_{вх}$ по первой гармонике входного сигнала:

$$K = \frac{S_{21}}{1 - S_{22}\Gamma_н}, \quad \Gamma_{вх} = S_{11} + \frac{S_{21}S_{12}\Gamma_н}{1 - S_{22}\Gamma_н}. \tag{1}$$

Таким образом, ни один из S-параметров не подлежит восстановлению из уравнений (1). Однако эту задачу можно решить, подключив внешнюю нагрузку $Z_н$ к нелинейному элементу, окруженному фильтрами, через достаточно длинный отрезок линии передачи и измерить входной комплексный коэффициент отражения ρ_1 и коэффициент прямой передачи или преобразования ρ_2 этого соединения.

При такой схеме измерения, каждую величину ρ_1 или ρ_2 как функции частоты f можно представить следующим образом:

$$\rho(f) = \sum_{n=0}^{N} \Phi_n(f)\left(e^{-i4\pi f\tau}\right)^n. \tag{2}$$

Если время задержки волны τ, создаваемое линией передачи, достаточно велико, то любая из функций $\Phi_n(f)$, связанная какими-либо соотношениями с искомыми S-параметрами, будет медленной по сравнению быстро осциллирующими множителями $(e^{-i4\pi f\tau})^n$, $n \geq 1$. Величина τ определяет частоты так называемых пространственных гармоник $n\tau$ в (2).

Задачу восстановления S-параметров в пределах выделенного «частотного окна» можно решить, используя представление искомых величин как функций f_k и коэффициента отражении от внешней нагрузки $\Gamma_{вых}$ в виде моделей линейной регрессии:

$$\begin{aligned}
&\mathrm{Re}[S_{ij}(f_k, \mathrm{Re}(\Gamma_{вых}), \mathrm{Im}(\Gamma_{вых}))] = x_1 + (f_k - f_1)x_2 + x_3\mathrm{Re}\Gamma_{вых}(f_k) + x_4\mathrm{Im}\Gamma_{вых}(f_k),\\
&\mathrm{Im}[S_{ij}(f_k, \mathrm{Re}(\Gamma_{вых}), \mathrm{Im}(\Gamma_{вых}))] = y_1 + (f_k - f_1)y_2 + y_3\mathrm{Re}\Gamma_{вых}(f_k) + y_4\mathrm{Im}\Gamma_{вых}(f_k),
\end{aligned} \tag{3}$$

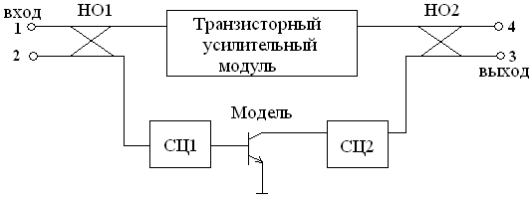
$$\Gamma_{вых}(f_k) = \Gamma_н e^{-i4\pi f_k\tau}.$$

Величина $\Gamma_н$ в выражении (3) для $\Gamma_{вых}$ представляет собой коэффициент отражения, создаваемый отражающей нагрузкой и входным импедансом вентиля. Обе

эти величины и $\Gamma_н$ и $\Gamma_{вых}$ на всех частотах, используемых для восстановления искомых параметров, можно измерить измерительным преобразователем. Величину задержки τ также можно определить с высокой точностью из результатов измерений.

Восстановленные S-параметры в режиме большого сигнала, можно использовать в задаче идентификации параметров нелинейной модели транзистора или диода. Успех решения задачи зависит от того, насколько результаты испытаний объекта анализа соответствуют реальным условиям его применения. Поэтому, целесообразно измерять параметры не транзистора, а реального усилительного модуля.

Идея идентификации состоит в использовании свойств балансной схемы усилителей см. рисунок. Первый канал балансной схемы содержит транзисторный усилительный модуль, описываемый элементами волновой матрицы рассеяния, измеренными на заданных частотах. Второй канал образован согласующими цепями транзисторного усилительного модуля СЦ1 и СЦ2 и моделью транзистора в виде эквивалентной схемы. Согласующие цепи также описываются волновыми параметрами рассеяния.



В случае, когда модель, идентична реальному транзистору, вход и выход балансной схемы идеально согласованы, а все остальные выходы попарно развязаны.

Использование идеальных квадратурных направленных ответвителей позволяет наблюдать S-параметры (реальные и мнимые части отдельно) всей схемы как функции частоты, которые, в свою очередь, связаны с параметрами модуля и модели соотношениями:

$$S_{11}=S_{11\,\text{модуль}} - S_{11\,\text{модель}},\ S_{24}= S_{12\,\text{модуль}} - S_{12\,\text{модель}},$$

$$S_{41}= S_{21\,\text{модуль}} - S_{21\,\text{модель}},\ S_{33}= S_{22\,\text{модуль}} - S_{22\,\text{модель}}.$$

Если схемы усилителей идентичны, то $S_{11}=S_{41}=S_{24}=S_{33}=0$. Команды Tuner или Optimize (метод Pointer-Automatic Optimization) позволяют добиться выполнения этих равенств, при активизации параметров модели транзистора. Однако, ввиду несовершенства модели, следует стремиться к минимуму этих функций во всей полосе частот. Удается весьма существенно минимизировать разницу между S-параметрами усилительного модуля и его модели. Идентификация моделей диодов осуществляется аналогичным образом.

ДАТЧИКИ ПАРАМЕТРОВ ОКОЛОЗЕМНЫХ ФИЗИЧЕСКИХ ПРОЦЕССОВ НА ОСНОВЕ ОПОРНЫХ СИГНАЛОВ ГЛОБАЛЬНОЙ СИНХРОНИЗАЦИИ ПРИРОДНЫХ ЯВЛЕНИЙ

К.Г.Кирьянов [1], А.В.Пастухов [1], А.В.Шабельников [2]

[1] ФГУП ННИПИ «Кварц», [2] ИРЭ РАН РФ.

Выдающаяся заслуга в постановке и разработке проблемы влияния космических факторов на процессы, происходящие на Земле, принадлежит А.Л. Чижевскому, впервые высказавшему идею о тесной зависимости явлений, происходящих в биосфере, академику В.И. Вернадскому – создателю учения о биосфере [1,2]. В регулярно проходящих международных симпозиумах и конференциях обсуждаются корреляции биологических и физико-химических процессов с космическими и гелио-геофизическими факторами. В некоторых из этих работ упоминается о гравитационной природе влияния космофизических факторов на процессы, протекающие в земных условиях. Однако в них не приводится конкретных соотношений для оценки периодов колебаний в слабо зашумленных экспериментально регистрируемых данных, показывающих природу глобальной синхронизации естественных и антропогенных процессов, отмеченную в [3] и последующих работах автора.

Регистрируемые периоды, как правило, содержатся в множестве, определяемом набором (сеткой) периодов (гипотеза А.В.Шабельникова):

$$T(n,m)=T_1\bullet(1/n^2-1/m^2),\ \text{где } n=1,2,3,...;\ m=2,3,4,...,\ n<m, \qquad (1)$$

а T_1 (подробнее см., например, Инициативный отчет по НИР «Прогноз». ИРЭ РАН,1993 на тему «Исследование возможностей и разработка методов прогноза временных изменений параметров некоторых природных процессов на глобальном и региональном уровнях») является одним из важнейших физических параметров, характеризующих период «вынуждающего», «захватывающего» и синхронизирующего околоземные процессы движения со специфическими периодами T(n,m). Следует заметить, что формула (1) по виду напоминает выражение для частот излучения водородоподобных атомов [4], в которых вместо периодов фигурируют частоты излучения $\nu(n,m)$ спектральных серий, период T_1 заменяется на величину $\nu_0 = RCZ^2$, R – постоянная Ридберга, C – скорость света, Z – порядковый номер элементов периодической системы Менделеева.

Значения основных периодов T_1, обязанные вращению внешних по отношению к Земле тел и в квазистационарном режиме жестко связанны между собой, и зависят от сил гравитационного взаимодействия, определяемых для каждой пары тел. Сложная квазистационарная динамика движения планет определяется собственными периодами вращения тел, каждый из которых может являться источником и причиной наличия спектральных компонент, которые могут наблюдаться в экспериментальных данных при подходящих условиях (малый уровень шума, удачная ориентация объекта, время суток и т.д.). Опуская обсуждение соотношений, связывающих между собой значения основных периодов T_1 вращающихся тел или их групп (см.[3]), укажем лишь важнейшие из них, часто встречающиеся

при спектральной обработке экспериментальных данных[5,6], и известные с большой точностью [7]:
1930 лет – период колебаний Солнечной активности;
178,8 лет – период движения Солнца вокруг центра Солнечной системы;
21,962года – один из периодов колебаний Солнечной активности;
11,199года (4090,8 суток) – самый известный период Солнечной активности;
1 год (365, 256 суток) – годичный период;24 часа (1440 мин.) – суточный период;
И т.д.

Простейшие спектральные компоненты, обнаруживаемые при обработке приведенных ниже данных, соответствую частному случаю формулы (1) со значением $m = \infty$:

$$T(n,\infty)=T_1 \cdot 1/n^2 \qquad (2)$$

Результаты спектральной обработки экспериментальных околоземных процессов опубликованные в более чем трёх десятках публикаций авторов настоящей работы(см., например, ссылки в инициативной НИР - «Комплексный анализ спектров временных колебаний параметров некоторых природных процессов и поиск спектральных аналогий между ними»// Заключительный отчет. Шифр-Спектр-3, ИРЭ РАН. Декабрь, 2003 г, 40 с.) подводят к идее использования глобальной синхронизации для построения весьма чувствительных измерительных датчиков и измерительных приборов околоземных физических процессов.

Обнаружены экспериментально каналы и способы воздействия не гравитационного характера на характеристики приборов, например, формирующих полосу пропускания канала наблюдения параметров сеток (1) и (2) периодов (частот), модулирующих, изменяющих пропорционально параметры сеток (амплитуд, фаз, и др.). Точность измерения датчиков и приборов будет определяться, в основном,

- "установкой нуля" измерительного датчика, зависящей от точности T_1 (порядка $\sim 10^{-8}$ [7]) и подобранных параметров сетки n и m, входящих в формулы (1) и (2),
- калибровкой шкал по заданному отклонению параметров сеток при других значениях параметров T_1, n или m, выбранных разработчиком датчиков.

Работа выполнена при частичной поддержке РФФИ (грант 02-02-17573).

[1] Вернадский В.И. Размышления натуралиста –М.: Наука, 1975.
[2] Чижевский А.Л. Земное эхо солнечных бурь. Изд.2-е –М.: Мысль, 1976.
[3] Шабельников А.В. Единая космическая ритмика Вселенной. // Космические циклы и ритмы жизни. Серия «Биология». М.: Знание, 1981, № 8, с.12.
[4] Зоммерфельд А. Строение атома и спектры - М.: ГИТТЛ, 1956**.**
[5] Кирьянов К.Г., Шабельников А.В. //Радиотехника и электроника. 1995,Вып.5, с.753.
[6] Кирьянов К.Г., Шабельников А.В.. К природе глобальной синхронизации естественных и антропогенных процессов. Вестник ВВО АТН РФ,N3 1997,с.30.
[7] Ален К.У. Астрофизические величины. –М.: Мир, 1977г., с.35.

ПРИНЦИП ДИНАМИЧЕСКОЙ КОМПЕНСАЦИИ Г.В. ЩИПАНОВА И МАТЕМАТИЧЕСКИЕ МОДЕЛИ КРИПТОСИСТЕМ

А.А.Горбунов, К.Г.Кирьянов

Нижегородский госуниверситет

В работах Г.В. Щипанова впервые было предложено использовать принцип компенсации внешнего возмущающего воздействия на систему при синтезе систем автоматического регулирования (см. [1]). Щипановым были получены условия (равенство нулю характеристического минора в линеаризованной системе), при выполнении которых поведение соответствующей минору переменной системы становится независимым (*инвариантным*) относительно внешнего воздействия, действующего на один из входов системы ([1], с.399). Кроме того, в дальнейшем было показано, что «щипановские» системы «негрубы» относительно чистых запаздываний, т.е. при наличии сколь угодно малых чистых запаздываний система может оказаться неустойчивой ([1], с.414).

При построении математических моделей (ММ) криптосистем (КС) можно обнаружить их общие черты с системами стабилизации авиационных машин, рассматриваемые Щипановым. Одним из способов, позволяющих получать унифицированный вид ММ КС, является подход, основанный на описании блоков шифратора и дешифратора КС в виде q-уровневых линейных цифровых автоматов (ЛЦА) [2]. В настоящей работе на примере ММ ЛЦА демонстрируется возможность проявления эффекта компенсации в дискретных динамических системах (ДДС). При этом при синтезе ММ дискретных КС, не возникает, в отличие от непрерывных щипановских регуляторов, проблемы «негрубости», т.к. дискретные по уровню и времени КС «грубы» изначально.

Рассмотрим систему динамических (т.е. в зависимости от типа используемой алгебраической структуры (АС) – дифференциальных, разностных и т.д.) уравнений для 3-х функций времени $x_1(t)$, $x_2(t)$, $x_3(t)$:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = u(t) \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = 0 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = 0 \end{cases} . \qquad (1)$$

Здесь динамические операторы $a_{ij} = B_{ij}p - C_{ij}$ – не выше первого порядка, B_{ij}, C_{ij} – числовые элементы соответствующей АС, p – символ динамики, являющийся, например, оператором дифференцирования для множества действительных чисел $\boldsymbol{R}$, разностным оператором для множеств дискретных элементов ($\boldsymbol{Z}$, $GF(q)$ и др.)

Условия инвариантности Г.В. Щипанова функции $x_1(t)$ относительно воздействия $u(t)$ запишутся как:

$$\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} = a_{22}a_{33} - a_{23}a_{32} = 0 ,$$

откуда имеем:
$$\begin{cases} B_{22}B_{33} - B_{23}B_{32} = 0 \\ B_{22}C_{33} + B_{33}C_{22} - B_{23}C_{32} - B_{32}C_{23} = 0 \\ C_{22}C_{33} - C_{23}C_{32} = 0 \end{cases}. \qquad (2)$$

Для приведения системы уравнений (1) к форме Коши нужно, рассматривая ее как систему линейных *алгебраических* уравнений относительно неизвестных px_1, px_2, px_3, разрешить ее относительно этих неизвестных.

$$\left\{ \begin{bmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{bmatrix} \cdot \begin{bmatrix} px_1 \\ px_2 \\ px_3 \end{bmatrix} = \begin{bmatrix} C_{11}x_1 + C_{12}x_2 + C_{13}x_3 + u \\ C_{21}x_1 + C_{22}x_2 + C_{23}x_3 \\ C_{31}x_1 + C_{32}x_2 + C_{33}x_3 \end{bmatrix} \right. . \qquad (3)$$

Из требования разрешимости системы (3) к имеющимся условиям инвариантности (2) добавляется также следующее условие:

$$\begin{vmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{vmatrix} \equiv |B| \neq 0 . \qquad (4)$$

В результате, система динамических уравнений (1), сведенная к форме Коши, принимает вид:

$$\begin{bmatrix} px_1 \\ px_2 \\ px_3 \end{bmatrix} = A_K \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + B_K \cdot u \ . \qquad (5)$$

В случае дискретной динамической системы (ДДС) получаем:

$$\bar{x}(t + \Delta t) = \tilde{A}\bar{x}(t) + \tilde{B}u(t), \quad \text{где: } \tilde{A} = \left[I + \Delta t A_K \right], \ \tilde{B} = \left[\Delta t B_K \right]. \qquad (6)$$

Был проведен компьютерный эксперимент по моделированию работы ЛЦА в АС $GF(q)$, значения параметров которых удовлетворяют условиям инвариантности (2), а также условию (4). Результаты эксперимента над данными ДДС подтверждают идентичность поведения переменной $x_1(t)$ как в случае автономного режима работы ЛЦА ($u(t)\equiv 0$), так и в случае неавтономного режима.

Таким образом:

- установлена родственность требований стабилизации в системах автоматического регулирования и восстановления сигнала в КС;
- показана возможность проявления эффекта компенсации в ДДС;
- характер компенсации в подобных ДС имеет точный характер в силу свойства дискретности состояний.

[1] Г.В. Щипанов и теория инвариантности (Труды и документы). Составители З.М. Лезина, В.И. Лезин. М.: Изд-во физико-математической литературы, 2004.

[2] Горбунов А.А., Кирьянов К.Г. // В кн.: Вестник ННГУ им. Н.И. Лобачевского. Серия «Радиофизика». Вып. 1(2). Н. Новгород: Изд-во ННГУ, 2004, с.24.

ВОССТАНОВЛЕНИЕ ПРОПУСКОВ В КОМПЬЮТЕРНЫХ 2 D ИЗОБРАЖЕНИЯХ

А.В.Грачев

Нижегородский госуниверситет

Почти всегда, при передаче изображения с помощью сетей, не предусматривающих подтверждение принятой информации (например, передача изображений с помощью факсов или телевидения), наблюдается шум типа «снег». Чем хуже линия передачи или слабее сигнал, тем интенсивность такого шума больше. В работе [1] описывались методы восстановления пропусков в экспериментальных данных с использованием равномерной и неравномерной временных сеток. В данной работе использован метод неравномерной временной сетки, где в качестве временного ряда взята пространственная координата – порядковый номер пикселя в столбце матрицы изображения. Восстанавливается же интенсивность пикселя, которая может принимать значения от 0 до 255 (0 – черный цвет, 255 – белый). В работе считается шумом пиксель со значением 255, но можно установить и другой порог восстановления. Восстановление проведено методами ряда Котельникова и сплайн-интерполяции пакета MathCad 2000 Pro.

Подготовка изображения к восстановлению одинакова для обоих методов и заключается в следующем:

- Из столбцов матрицы изображения размером MxN пикселей удаляются пиксели со значением 255. Соседние пиксели смещаются на их позицию. После данной процедуры некоторые столбцы окажутся короче количества строк M.
- В концы «коротких» столбцов добавляются значения отличные от диапазона 0 – 255, например -1. Это необходимо для облегчения компьютерных расчетов. Таким образом, снова получим матрицу MxN.
- Параллельно формируем матрицу порядковых номеров пикселей отличных от 255, дополняя столбцы до размера M значениями –1.

В итоге получается две матрицы размером MxN – матрица №1 значений интенсивности изображения и соответствующая ей матрица порядковых номеров №2.

Интерпретация ряда Котельникова применительно к изображению:

$$s(t) = \sum_{k=0}^{K-1} y_k \frac{\sin\left[\omega\left(t - \frac{T_k\pi}{\omega}\right)\right]}{\omega\left(t - \frac{T_k\pi}{\omega}\right)}, \qquad (1)$$

где $\omega = 2\cdot\pi\cdot fv$,

fv – будет означать частоту следования порядковых номеров пикселей исходного изображения, например для 0, 1, 2, 3, …,K – *fv* будет равна 1,

T – столбец матрицы неравномерного времени (порядковые номера существующих пикселей),
y – значения интенсивностей из матрицы №1,
K – количество элементов в столбце матрицы №1 отличных от –1.

Восстановление будет произведено с использованием ряда Котельникова по формуле (1), а также при помощи математического пакета MathCad 2000 Professional, который представляет разнообразные функции кубичной сплайн-интерполяции. В данной работе были использованы функции lspline и interp.

Для компьютерного эксперимента был взят файл изображения в формате bmp размером 100x100 пикселей. Искусственным путем в изображение был добавлен шум, включением белого пикселя с вероятностью 0,1. Исходное и зашумленное изображения приведены на рисунках:

Восстановленные изображения:

Изображение восстановлено с помощью ряда Котельникова

Изображение восстановлено с помощью сплайн-интерполяции

Оба метода дали удовлетворительное качество восстановления пропусков.

Следует отметить, что в отличие от сплайн-интерполяции, точность восстановления с использованием ряда Котельникова повышается с ростом числа вовлекаемых в восстановление членов ряда, т.к. в восстановлении участвует также и частотная составляющая изображения. Этот же метод создания неравномерной временной сетки можно использовать для ресамплинга изображений – изменения размеров изображения, в т.ч. для некратного увеличения или уменьшения изображения.

[1] Грачев А.В. //В кн.: Вестник ННГУ –Н. Новгород, 2004, с.15.

К ВОПРОСУ ОБ АНАЛИЗЕ ХЭШ-ФУНКЦИЙ НА СТОЙКОСТЬ К КОЛЛИЗИЯМ

А.С.Бажухин

Нижегородский госуниверситет

В современных информационных технологиях широко используются хэш-функции. Они используются в системах аутентификации, а также при формировании ЭЦП. Хэш функции (X→Y=H(X)), которые испольются в криптографии должны обладать следующими свойствами:

1. Хэш-функция H должна применяться к блоку данных любой длинны.
2. Хэш-функция H создаёт выход фиксированной длинны.
3. Значение H(X) относительно легко вычисляется для любого значения X
4. Для любого данного значения Y, вычислительно невозможно найти X, что H(X)=Y (preimage resistance).
5. Для любого данного Z вычислительно невозможно найти X≠Z, что H(X)=H(Z) (second preimage resistance).
6. Вычислительно невозможно найти произвольную пару X≠Z, что H(X)=H(Z) (collision resistance)[1].

Вообще, современная литература подразделяет всевозможные хэш-функции на три класса:

1. Построенные на основе известных вычислительно сложных математических задач.
2. Построенные на основе алгоритмов шифрования (предполагается, что шифратор стойкий).
3. Построенные «с нуля».

Существуют методы анализа хэш-функций на стойкость к коллизиям (св-во 6). Однако в связи с большим разнообразием существующих хэш-функций, существует множество методов анализа, т.к. универсальные методы анализа, применимые ко всем существующим хэш-функциям существуют следующие:

1. Метод случайного перебора
2. Метод основанный на «парадоксе дней рождений»

Первый метод на практике не применяется в силу своей чрезвычайно большой ресурсоёмкости. Второй применяется для хэш-функций, выходное значение которых невелико (так для хэш-функций с длинной выходного значения n бит необходимо сгенерировать $2^{n/2}$ псевдослучайных входных значений, для того, чтобы вероятность коллизии была ≈0,5) [2]. Похожие идеи реализованы в алгоритме предложенном в [3].

Соответственно, разработка алгоритма анализа хэш-функций, независимого от типа хэш-функции, является важной задачей. Предложен алгоритм анализа, базирующийся на том, что появление различных символов и блоков символов в значение хэш-функции не равновероятно. Используется математическая модель хэш-функции, предствленая с внутренней стороны структурой S, вектором параметровY$\{y_1...y_L\}$, где y_i – i-й символ значения хэш-функциия, A_H – алфавит хэш-

хэш-функции. С внешней стороны хэш-функция представлена набором критериев качества функционирования $K_C=\sum P_C(y_i)$ – критерий символьной вероятности, $K_П=\sum P_П(y_i,i)$ – критерий позиционной вероятности, $K_S=\sum P_S(y_i, y_{i+1}... y_{i+s-1})$ - критерий вероятности для s символьных блоков. Целевая функция может быть построена как в аддитивном, так и в мультипликативном виде. Целевая функйия, будучи примененой к конкретному значению хэш-функции означает насколько вероятно встретить такое же (или похожее) значение. Далее задаётся пороговое значение, которое позволяет отсекать из рассмотрения «маловероятные» значения хэш-функции. Данный алгоритм был опробован на хэш-функции crypt(), которая используется в системе аутентификации ОС семейства UNIX. В результате работы полных совпадений небыло найдено (что можно обьяснить выбором относительно небольшого множества входных значениий), однако были найдена совпадения в 7 символах из 11. Было проанализировановлияние различных парамаетров (порогового значения, весовых коэффициентов, вида целевой функции) на работу алгоритма. По результатам можно отметить, что данный алгоритм не всегда позволяет найти коллизии, но позволяет указать подмножество множества входных значений, в которых коллизии не будет. Данный метод применим к любым хэш-функциям, независимо от их типа.

На данный момент существует ряд работ, в которых предложены методы анализа хэш-функций, основанных на алгоритмах шифрования, позволяющие находить коллизии вида $H(M)=H(M+\Delta M)$, где M – входное сообщение, а ΔM разница между двумя сообщениями, при которыми возможны коллизии [4,5,6].

Таким образом на настоящее время аппарат анализа существующих хэш-функция на стойкость к коллизиям довольно быстро совершенствуется, в связи с чем перспективным направлением развития хэш-функция можно считать разработку хэш-функций на основе континуальных динамических систем.

[1] Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С.:2-е издание.
[2] Yuval G., How to swindle Rabin, Cryptologia, v. 3, N 3, 1979, p187.
[3] Quisquater J.-J., Delescaille J.-P., How easy is collision search? Application to DES, Proc. EUROCRYPT'89, p429, Quisquater J.-J., Delescaille J.-P., How easy is collision search. New results and applications to DES, Proc. CRYPTO'89, Lect. Notes in Comput. Sci., v. 435, 1990, 408p.
[4] Biham E., Shamir A., Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI and Lucifer, Proc. CRYPTO'91, Lect. Notes in Comput. Sci., v. 576, 156p.
[5] Biham E., Chen R., Near-Collisions of SHA-0.
[6] Joux A., Multicollisions in iterated hash functions. Application to cascaded constructions.